

Novel representation of discrete n -D autonomous systems

Debasattam Pal *

Harish K. Pillai †

Abstract

In this paper we address the problem of representing solutions of a system of scalar linear partial difference equations akin to state space equations of 1-D systems theory. We first obtain a representation formula for a special class of autonomous systems. Then we show every autonomous system can be converted into the special ones by a coordinate transformation on \mathbb{Z}^n . Using this conversion we provide representation formula for general autonomous systems. The representation formula we present can be viewed as multidimensional flow operators acting on initial conditions. These initial conditions are required to satisfy certain compatibility conditions. We give a full description of the set of allowable initial conditions.

In our search for a general representation formula, one algebraic result plays a very crucial role. In this result we show that every quotient ring of the n -variable Laurent polynomial ring can be made a finitely generated faithful module over another Laurent polynomial ring of smaller dimension by doing a suitable change of coordinates. We call this result a discrete version of Noether's Normalization Lemma.

1 Introduction

One of the most crucial discoveries in the theory of dynamical systems is the notion of *state variables*. The state variables serve, simultaneously, two purposes in the analysis and control of dynamical systems. On the one hand, they relate to the system's memory, or, equivalently, energy storing capability, while on the other hand, they provide a recursive formula to compute the trajectories in the systems. The hallmark characteristic of state variables that enables the above-mentioned two benefits is that the representation of a dynamical system in state variables is a *first order* ordinary differential equation (ODE) of the following form:

$$\frac{dx}{dt} = f(x, u), \quad y = h(x, u). \quad (1)$$

For discrete dynamical systems, that is, systems described by ordinary difference equations (odes), the state equation takes the form:

$$x(k+1) = f(x(k), u(k)), \quad y(k) = h(x(k), u(k)). \quad (2)$$

Given the benefits of state variables it is desirable to have systems described in the form of equation (1). Unfortunately, often the first principles modelling of dynamical systems end up giving higher order equations [RW97]. However, for a system of ODEs, a higher order mathematical model can always be *reduced* to a state variable model (see [RW97] where this was proven for linear time-invariant systems). And, therefore, it is a standard practice to consider dynamical systems already given by a state variable model.

*Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Guwahati - 781 039, India. debasattam@iitg.ernet.in,

†Department of Electrical Engineering, Indian Institute of Technology Bombay, Mumbai - 400 076, India. hp@ee.iitb.ac.in

The situation drastically changes when it comes to systems described by partial differential/difference equations (PDEs/pdes). For such n -D systems¹, as they are often called, it is not clear whether a state variable representation similar to equations (1) or (2) always exists. The main hindrance in obtaining such a first order representation for n -D systems is that, unlike 1-D systems, there is no fixed direction of evolution for n -D systems. This problem can be somewhat overcome by letting one of the independent variables play the role of ‘time’ (see, for example, [CZ95, STW02, NRR11]). This approach naturally leads to an infinite dimensional state space [CZ95]. A serious drawback of this approach is that there are many n -D systems for which such a state space representation with a special variable treated as time may not even be possible [NRR11].

In this paper, we show that for *every* discrete n -D autonomous system, a first order representation akin to equation (2) can be obtained. Our inspiration comes from the special class of autonomous n -D systems – the *strongly autonomous systems*. It is known that a strongly autonomous linear n -D system admits a first order representation of the following type:

$$\left. \begin{aligned} x(\nu_1 + 1, \nu_2, \dots, \nu_n) &= A_1 x(\nu_1, \nu_2, \dots, \nu_n) \\ x(\nu_1, \nu_2 + 1, \dots, \nu_n) &= A_2 x(\nu_1, \nu_2, \dots, \nu_n) \\ &\vdots \\ x(\nu_1, \nu_2, \dots, \nu_n + 1) &= A_n x(\nu_1, \nu_2, \dots, \nu_n) \\ w(\nu_1, \nu_2, \dots, \nu_n) &= C x(\nu_1, \nu_2, \dots, \nu_n), \end{aligned} \right\} \quad (3)$$

where A_1, A_2, \dots, A_n are real square invertible matrices, C is a real matrix of appropriate size [RW89, FRZ93]. Note that here, each state matrix A_i encodes the information about the evolution of the state variable x in the i^{th} direction of the integer grid \mathbb{Z}^n , over which the system’s trajectories evolve. The state variable x evaluated at any integer n -tuple $(\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$ is a finite dimensional vector. So the state space here is a finite dimensional vector space. We show in this paper, that for a class of systems (that strictly contains the class of strongly autonomous systems), such a first order representation exists. However, the representation has a striking difference from equation (3): here the state space is usually infinite dimensional. We show that for these systems, there exists a non-negative integer $d < n$ such that the state space is a subspace of the space of all vector valued discrete trajectories evolving over \mathbb{Z}^d (we call such trajectories d -D trajectories). And, the first order representation provides an $(n - d)$ -D evolution on the state space. Interestingly, as we show in this paper, the number d is equal to a geometric invariant of the autonomous system: it equals the dimension of the *characteristic variety* of the system. As a result of this, the representation of equation (3) turns out to be a special case, because the defining property of strongly autonomous systems is that the dimension of their characteristic varieties is zero, therefore, $d = 0$ in this case, and so the state space turns out to be finite dimensional.

We call this special class of autonomous systems *strongly relevant of order d* . The characterizing property of this class is a certain algebraic property. The crucial benefit of this algebraic characterization is that every discrete n -D autonomous system can be transformed in to an ‘equivalent’ strongly relevant system by a change of coordinates in \mathbb{Z}^n . This enables us to provide a first order representation for *any* discrete autonomous n -D system. A crucial role in this transformation is played by a normalization process, which we call the discrete Noether’s normalization lemma (DNNL), for it is an analogue, applied to Laurent polynomial rings, of the classical Noether’s normalization lemma, which is applied to polynomial rings.

The above-mentioned first order representations can be utilized to provide explicit solution formulae for a given discrete autonomous n -D system. We provide these formulae as algorithms for solving system of autonomous pdes in this paper. Interestingly, a parallel can be drawn between these representation formulae and the classical result of Ehrenpreis-Palamodov integral

¹This way, systems described by ODEs/odes are called 1-D systems.

representation theorem for continuous autonomous n -D systems [Bjö79, Obe90, Stu02]. The integral representation formula can be viewed as an evolutionary equation of initial conditions specified on the characteristic variety (which is a d -D object in \mathbb{C}^n). The representation formulae of this paper, too, are evolutionary equations on state spaces, which are subspaces of d -D trajectories. However, a striking difference is that, in our case, since the state space is just a subspace of d -D trajectories, the initial conditions are specified over \mathbb{Z}^d as opposed to the ones specified over the characteristic variety in the integral representation theorem. Further, our evolutionary equation does not involve an explicit integration. These two facts make our representation formulae easily implementable on a computer.

The results presented in this paper are generalizations of those in [PP13], which deals with the special case of $n = 2$. It is well-known that often such an extension from $n = 2$ to a general n is not straight-forward, owing to the fact that dimension 2 algebras have certain special features that do not carry over to algebras with higher dimensions (see [PS98] for some of these special features of 2-variable polynomial rings). In our case, the main difficulty arises in obtaining the DNNL for higher dimensional rings. Another crucial difference between 2-D and n -D is that, in case of general n , the number d can be anything between 0 and $n - 1$, while in case of 2-D the number d can only be 0 or 1.

The paper is organized in the following manner: in the next section (Section 2) we discuss the notation used in this paper, and provide some preliminaries required for the main subject matter of the paper. Then, in Section 3, we consider a special class of discrete autonomous n -D systems and show how a first order representation of such systems can be obtained. Using this representation we then provide an explicit solution formula, alongwith an algorithm, to compute the trajectories in such systems. In Section 4 we state and prove the discrete Noether's normalization lemma. Then using this normalization we provide, in Section 5, a first order representation for general autonomous discrete n -D systems. As a consequence, we provide an explicit solution formula for trajectories in general autonomous discrete n -D systems, and also an algorithm to compute them. Finally, in Section 6 we provide some interesting insights on the set of allowable initial conditions that are used in the solution formulae.

2 Notation and preliminaries

2.1 Notation

We use \mathbb{R} and \mathbb{C} to denote the fields of real and complex numbers, respectively. Consequently, \mathbb{R}^n , \mathbb{C}^n denote the n -dimensional vector spaces over \mathbb{R} and \mathbb{C} , respectively. The set of integers is denoted by \mathbb{Z} , and \mathbb{Z}^n denotes the set of n tuples of elements in \mathbb{Z} . In this paper, our main object of study is a particular class of multiply indexed sequences of elements in \mathbb{R}^q , for some positive integer q . We denote the set of sequences in \mathbb{R} indexed by \mathbb{Z}^n by the symbol \mathcal{W} , *i.e.*, $\mathcal{W} := \{w : \mathbb{Z}^n \rightarrow \mathbb{R}\}$. To denote the set of vector valued sequences indexed by \mathbb{Z}^n , we use \mathcal{W}^q , *i.e.*, $\mathcal{W}^q := \{w : \mathbb{Z}^n \rightarrow \mathbb{R}^q\}$. The Laurent polynomial ring in n indeterminates $\sigma_1, \sigma_2, \dots, \sigma_n$, usually written as $\mathbb{R}[\sigma_1^{\pm 1}, \sigma_2^{\pm 1}, \dots, \sigma_n^{\pm 1}]$, will be denoted, in this paper, by \mathcal{A} , and the same in the first d indeterminates $\sigma_1, \sigma_2, \dots, \sigma_d$, written as $\mathbb{R}[\sigma_1^{\pm 1}, \sigma_2^{\pm 1}, \dots, \sigma_d^{\pm 1}]$, will be denoted by \mathcal{A}_d . We use \mathcal{A}^q to denote the free module of rank q over \mathcal{A} , where the elements of \mathcal{A}^q are q -tuples written as row-vectors. For a set S , we use $S^{m \times n}$ to denote the set of $(m \times n)$ matrices with entries from the set S . We often use $\text{col}(\bullet)$ to stack up entries one above the other to make a column vector. The single letter σ is often used to denote the n tuple $(\sigma_1, \sigma_2, \dots, \sigma_n)$. Further, for an integer n tuple $\nu = (\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$, the symbol σ^ν denotes the monomial $\sigma_1^{\nu_1} \sigma_2^{\nu_2} \dots \sigma_n^{\nu_n}$. In this paper, we follow the bar notation to denote equivalence classes: for $r(\sigma) \in \mathcal{A}^q$ and a submodule $\mathcal{R} \subseteq \mathcal{A}^q$, we use $\overline{r(\sigma)}$ to denote the equivalence class of $r(\sigma)$ in the quotient module $\mathcal{A}^q/\mathcal{R}$.

2.2 Discrete n -D systems

By discrete n -D systems, in this paper, we mean systems described by a set of n -D linear partial difference equations with constant real coefficients. Such partial difference equations are often described using the n -D shift operators $\sigma_1, \sigma_2, \dots, \sigma_n$. These shift operators act on the n -D discrete ‘trajectories’ (i.e., real valued sequences indexed by \mathbb{Z}^n) $w \in \mathbb{R}^{\mathbb{Z}^n}$ as follows: for $\nu' := (\nu'_1, \nu'_2, \dots, \nu'_n), \nu := (\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$

$$(\sigma^{\nu'} w)(\nu) = w(\nu + \nu'), \quad (4)$$

where the sum $\nu + \nu'$ is the standard element-wise sum: $\nu + \nu' = (\nu_1 + \nu'_1, \nu_2 + \nu'_2, \dots, \nu_n + \nu'_n)$. This definition can be extended naturally to define the action of \mathcal{A} , the Laurent polynomial ring in the shifts, on \mathcal{W} . And, likewise, a row-vector $r(\sigma) = [r_1(\sigma), r_2(\sigma), \dots, r_q(\sigma)]$ and a column-vector $w = \text{col}(w_1, w_2, \dots, w_q) \in \mathcal{W}^q$ we define $r(\sigma)w := \sum_{i=1}^q r_i(\sigma)w_i$. This defines the action of the row module \mathcal{A}^q on \mathcal{W}^q .

In this paper, as a convention, we always consider a vector valued trajectory as a column vector. Consequently, any tuple of difference operators that act on a column vector of trajectories and produces scalar trajectories, is written as a row, so that this action can be compactly written as a ‘dot’ product of a tuple of difference operators and that of trajectories. So, as a convention, in this paper, elements from a module over an operator ring \mathcal{A} (or \mathcal{A}_d , as the case might be) are assumed to be row vectors.

2.3 The kernel representation

Following Willems’ 1-D terminology [Wil91], we call the collection of trajectories $w \in \mathcal{W}^q$ that satisfy a given set of partial difference equations the *behavior* of the system, and denote it by \mathfrak{B} . The above description of the action of \mathcal{A}^q on \mathcal{W}^q gives the following representation of behaviors of discrete n -D systems:

$$\mathfrak{B} := \{w \in \mathcal{W}^q \mid R(\sigma)w = 0\}, \quad (5)$$

where $R(\sigma) \in \mathcal{A}^{\bullet \times q}$. The above equation (5) is called a *kernel representation* of \mathfrak{B} and written as $\mathfrak{B} = \ker(R(\sigma))$. Note that various different matrices can have the same kernel. Importantly, all matrices having the same row-span over \mathcal{A} result in the same behavior. This leads to the following equivalent definition of behaviors: let $R(\sigma) \in \mathcal{A}^{\bullet \times q}$ and $\mathcal{R} := \text{rowspan}(R(\sigma))$,

$$\mathfrak{B}(\mathcal{R}) := \{w \in \mathcal{W}^q \mid r(\sigma)w = 0 \text{ for all } r(\sigma) \in \mathcal{R}\}. \quad (6)$$

The submodule \mathcal{R} generated by the rows of a kernel representation matrix is called *the equation module* of \mathfrak{B} . It was shown in [Obe90] that the submodules of \mathcal{A}^q and discrete n -D behaviors that have q number of dependent variables (that is $w(\nu) \in \mathbb{R}^q$ for all $\nu \in \mathbb{Z}^n$) are in an inclusion reversing one-to-one correspondence with each other. We denote the set of all discrete n -D behaviors with q number of dependent variables by \mathfrak{L}^q .

In mathematical modelling of systems, it often turns out to be beneficial to incorporate auxiliary dependent variables called *latent variables* [Wil91]. A representation of the behavior involving both the variables of interest (the *manifest variables* [Wil91]) and the latent variables is called a latent variable representation. The following equation is one such representation:

$$\mathfrak{B} = \left\{ w \in \mathcal{W}^q \mid \exists \ell \in \mathcal{W}^{q'} \text{ such that } R(\sigma)w + M(\sigma)\ell = 0 \right\}. \quad (7)$$

Note that the state variables are a special type of latent variables.

2.4 Autonomous systems

In this paper, we deal with a special type of discrete n -D systems, namely *autonomous systems*. Among several equivalent definitions of n -D autonomous systems (see [FRZ93, PS98, Val01]), in this paper, we stick to the algebraic definition of [PS98], which we state below as Definition 1. In Definition 1 and later we need the notion of *characteristic ideal* of a discrete n -D system. Let the behavior \mathfrak{B} of a discrete n -D system be given by a kernel representation $\mathfrak{B} = \ker(R(\sigma))$ with $R(\sigma) \in \mathcal{A}^{\bullet \times q}$. The *characteristic ideal* of \mathfrak{B} , denoted by $\mathcal{I}(\mathfrak{B})$, is defined as the ideal of \mathcal{A} generated by the $(q \times q)$ minors of $R(\sigma)$. If the number of rows in $R(\sigma)$ is less than the number of columns q , then $\mathcal{I}(\mathfrak{B})$ is defined to be the zero ideal.

Definition 1. *A discrete n -D system is said to be autonomous if the characteristic ideal $\mathcal{I}(\mathfrak{B})$ is nonzero. Further, an autonomous behavior is said to be strongly autonomous if the quotient ring $\mathcal{A}/\mathcal{I}(\mathfrak{B})$ is a finite dimensional vector space over \mathbb{R} .*

2.5 The quotient module

Given a behavior $\mathfrak{B} = \ker(R(\sigma))$, let \mathcal{R} be the submodule of \mathcal{A}^q spanned by the rows of $R(\sigma)$. We define

$$\mathcal{M} := \mathcal{A}^q / \mathcal{R},$$

and call it the *quotient module* of \mathfrak{B} . This quotient module \mathcal{M} plays a central role in this paper. We often let elements from \mathcal{M} act on \mathfrak{B} . This action is defined as follows: for $m \in \mathcal{M}$, the action of m on $w \in \mathfrak{B}$ is defined to be the action of a lift of m in \mathcal{A}^q on w . For example, let $r(\sigma) \in \mathcal{A}^q$ be such that $\overline{r(\sigma)} = m \in \mathcal{M}$, then

$$mw := r(\sigma)w. \tag{8}$$

Note that m may have several distinct lifts in \mathcal{A}^q , but all of them have the same action on $w \in \mathfrak{B}$. This is because two lifts differ by an element in the equation module \mathcal{R} . Therefore, the action of this difference on any $w \in \mathfrak{B}$ produces the zero trajectory, for the action of any element in \mathcal{R} is zero on \mathfrak{B} . Thus, the definition of action of \mathcal{M} on \mathfrak{B} is well-defined.

Now note that it follows from Definition 1 above that \mathfrak{B} is autonomous *if and only if* the quotient module \mathcal{M} is a *torsion module*, i.e., for every $\overline{m(\sigma)} \in \mathcal{M}$ there exists a $f(\sigma) \in \mathcal{A}$ such that $\overline{f(\sigma)m(\sigma)} = 0 \in \mathcal{M}$. In that case we get the following ideal called the *annihilator ideal* of \mathcal{M} .

$$\text{ann}(\mathcal{M}) := \{f(\sigma) \in \mathcal{A} \mid f(\sigma)m = 0 \text{ for all } m \in \mathcal{M}\}.$$

3 A special case: \mathcal{M} is a finitely generated module over a smaller ring

We first consider a special case. Let the n -tuple of shift operators be partitioned into two tuples: $\sigma = (\sigma_1, \sigma_2)$, where $\sigma_1 = (\sigma_1, \sigma_2, \dots, \sigma_d)$ and $\sigma_2 = (\sigma_{d+1}, \sigma_{d+2}, \dots, \sigma_n)$. In this section, we consider the case when the quotient module \mathcal{M} happens to be *finitely generated* as a module over the subring $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$ (that is, the Laurent polynomial ring generated by the d -tuple of shift operators σ_1). We denote this smaller ring by \mathcal{A}_d .

The motivation for considering this special case comes from the intention to mimic the construction of states for strongly autonomous systems. Recall that, for strongly autonomous systems, the quotient module \mathcal{M} happens to be a finite dimensional vector space over \mathbb{R} . It is already well-known that, in that case, the n -D behavior admits a state-space representation of the form given by equation (3) (see []). However, there are many n -D autonomous systems that are not strongly autonomous. For such systems the quotient module is an infinite dimensional vector space over \mathbb{R} . Among these systems, there is a special class, for which \mathcal{M} is a finitely

generated module over a smaller ring \mathcal{A}_d . We formally define such systems as *strongly relevant system of order d* .

Definition 2. Let $\mathfrak{B} \in \mathfrak{L}^q$ be an autonomous system. Then \mathfrak{B} is said to be strongly relevant of order d if the quotient module \mathcal{M} of \mathfrak{B} is a finitely generated module over \mathcal{A}_d .

For example, the following scalar 2-D system

$$\mathfrak{B} = \ker \begin{bmatrix} \sigma_2^2 - 2\sigma_2 + 1 \\ \sigma_1\sigma_2 - \sigma_2 - \sigma_1 + 1 \end{bmatrix}$$

is a strongly relevant system of order 1. On the other hand, the scalar 2-D system

$$\mathfrak{B} = \ker [\sigma_1\sigma_2 - \sigma_2 - \sigma_1 + 1]$$

is *not* strongly relevant of any order. Note that a strongly relevant system of order 0 is nothing but a strongly autonomous system.

The assumption that \mathcal{M} is a finitely generated module over \mathcal{A}_d guarantees the existence of certain matrices which will be crucially used in obtaining the desired representation formulae. We describe the construction of these matrices and their properties below.

3.1 The matrix of relations, $X(\sigma_1)$

The quotient module \mathcal{M} being finitely generated over \mathcal{A}_d implies that we can find a finite collection of elements from \mathcal{M} , say $\{g_1, \dots, g_r\}$, that generate \mathcal{M} as an \mathcal{A}_d -module. This choice of generators gives us a surjective \mathcal{A}_d -module morphism

$$\begin{aligned} \psi : \mathcal{A}_d^r &\twoheadrightarrow \mathcal{M} \\ e_i &\mapsto g_i \end{aligned} \tag{9}$$

for $1 \leq i \leq r$, where e_i is the i^{th} standard basis row-vector

$$e_i = \begin{bmatrix} 0 & 0 & \cdots & 1 & \cdots & 0 \end{bmatrix} \in \mathcal{A}_d^r.$$

\uparrow
 i^{th} position

Clearly, $\ker(\psi)$ is a submodule of \mathcal{A}_d^r . Since \mathcal{A}_d^r is a Noetherian module, this submodule is finitely generated. Therefore, we can find a matrix $X(\sigma_1) \in \mathcal{A}_d^{k \times r}$ whose rows generate $\ker(\psi)$ as an \mathcal{A}_d -module. Thus \mathcal{M} turns out to be isomorphic as an \mathcal{A}_d -module with the quotient module $\mathcal{A}_d^r / \text{rowspan}(X(\sigma_1))$:

$$\mathcal{A}_d^r / \text{rowspan}(X(\sigma_1)) \simeq \mathcal{M} \text{ as } \mathcal{A}_d\text{-modules.} \tag{10}$$

We call $X(\sigma_1)$ a *matrix of relations* of the generators of \mathcal{M} as an \mathcal{A}_d -module.

3.2 Matrices representing the $(n - d)$ -tuple of shift operators $\sigma_{d+1}, \dots, \sigma_n$

Now consider the \mathcal{A}_d -module morphisms defined for $1 \leq j \leq (n - d)$ as

$$\begin{aligned} \mu_j : \mathcal{M} &\rightarrow \mathcal{M} \\ m &\mapsto \mu_j(m) := \sigma_{d+j} \cdot m. \end{aligned} \tag{11}$$

These maps are clearly \mathcal{A}_d -module morphisms. Since \mathcal{M} has been assumed to be finitely generated over \mathcal{A}_d , in order to specify these maps it is enough to specify their actions on the generators $\{g_1, \dots, g_r\}$. Suppose that for $1 \leq i \leq r$ and $1 \leq j \leq (n - d)$

$$\mu_j(g_i) = a_{i1,j}(\sigma_1)g_1 + a_{i2,j}(\sigma_1)g_2 + \cdots + a_{ir,j}(\sigma_1)g_r, \tag{12}$$

where $a_{i1,j}(\sigma_1), a_{i2,j}(\sigma_1), \dots, a_{ir,j}(\sigma_1) \in \mathcal{A}_d$. We denote by $A_j(\sigma_1)$ the following matrix

$$A_j(\sigma_1) = \begin{bmatrix} a_{11,j}(\sigma_1) & a_{12,j}(\sigma_1) & \cdots & a_{1r,j}(\sigma_1) \\ a_{21,j}(\sigma_1) & a_{22,j}(\sigma_1) & \cdots & a_{2r,j}(\sigma_1) \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1,j}(\sigma_1) & a_{r2,j}(\sigma_1) & \cdots & a_{rr,j}(\sigma_1) \end{bmatrix} \in \mathcal{A}_d^{r \times r}. \quad (13)$$

Equation (12) can now be written collectively for all i as

$$\mu_j \left(\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} \right) = A_j(\sigma_1) \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix}. \quad (14)$$

It then follows that multiplication by σ_{d+j} is represented by the matrix $A_j(\sigma_1)$. We prove this in the following lemma.

Lemma 3. *Suppose \mathcal{M} is a finitely generated module over \mathcal{A}_d . Let $\{g_1, \dots, g_r\} \subseteq \mathcal{M}$ be a generating set for \mathcal{M} as an \mathcal{A}_d -module. Consider $\psi : \mathcal{A}_d^r \rightarrow \mathcal{M}$ as given in equation (9). Further, for $1 \leq j \leq (n-d)$, let μ_j and $A_j(\sigma_1)$ be as defined by equations (11) and (13), respectively. Then the following diagram commutes.*

$$\begin{array}{ccc} \mathcal{A}_d^r & \xrightarrow{\psi} & \mathcal{M} \\ A_j(\sigma_1) \downarrow & & \downarrow \mu_j \\ \mathcal{A}_d^r & \xrightarrow{\psi} & \mathcal{M} \end{array} \quad (15)$$

where $A_j(\sigma_1) : \mathcal{A}_d^r \rightarrow \mathcal{A}_d^r$ is defined by right-multiplication by the matrix $A_j(\sigma_1)$ to the row-vectors in \mathcal{A}_d^r .

Proof : For any $r(\sigma_1) = [r_1(\sigma_1) \ r_2(\sigma_1) \ \cdots \ r_r(\sigma_1)] \in \mathcal{A}_d^r$ we want to show

$$\mu_j(\psi(r(\sigma_1))) = \psi(r(\sigma_1)A_j(\sigma_1)).$$

From the definition of the ψ map it follows that

$$\psi(r(\sigma_1)) = r_1(\sigma_1)g_1 + r_2(\sigma_1)g_2 + \cdots + r_r(\sigma_1)g_r. \quad (16)$$

Operating μ_j on both sides of equation (16) and then utilizing equation (14) we get

$$\begin{aligned} \mu_j(\psi(r(\sigma_1))) &= \mu_j(r_1(\sigma_1)g_1 + r_2(\sigma_1)g_2 + \cdots + r_r(\sigma_1)g_r) \\ &= [r_1(\sigma_1) \ r_2(\sigma_1) \ \cdots \ r_r(\sigma_1)] \mu_j \left(\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} \right) \\ &= [r_1(\sigma_1) \ r_2(\sigma_1) \ \cdots \ r_r(\sigma_1)] A_j(\sigma_1) \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} = \psi(r(\sigma_1)A_j(\sigma_1)). \end{aligned}$$

□

The matrices $A_1(\sigma_1), A_2(\sigma_1), \dots, A_{n-d}(\sigma_1)$ are called *companion matrices*. In the lemma below we list out some useful properties of these companion matrices.

Lemma 4. Consider ψ and μ_j , $A_j(\sigma_1)$, for $1 \leq j \leq (n-d)$, as defined by equations (9), (11) and (13), respectively. Then we have the following:

1. The matrices $A_1(\sigma_1), A_2(\sigma_1), \dots, A_{n-d}(\sigma_1)$ commute pairwise.
2. There exists a set of generators $\{g_1, g_2, \dots, g_r\}$ for \mathcal{M} as a module over \mathcal{A}_d such that each of the corresponding $A_j(\sigma_1)$'s is invertible in $\mathcal{A}_d^{r \times r}$ (that is, unimodular over \mathcal{A}_d).
3. With each of $A_j(\sigma_1)$'s invertible, we have the following commutative diagram for any $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$,

$$\begin{array}{ccc} \mathcal{A}_d^r & \xrightarrow{\psi} & \mathcal{M} \\ \left(\prod_{j=1}^{n-d} A_j(\sigma_1)^{\nu_j} \right) \downarrow & & \downarrow (\mu_1^{\nu_1} \circ \mu_2^{\nu_2} \circ \dots \circ \mu_{n-d}^{\nu_{n-d}}) \\ \mathcal{A}_d^r & \xrightarrow{\psi} & \mathcal{M} \end{array} \quad (17)$$

4. With each of $A_j(\sigma_1)$'s invertible, for every $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$, there exists a matrix $E(\sigma_1) \in \mathcal{A}_d^{k \times k}$ such that

$$X(\sigma_1) \left(\prod_{j=1}^{n-d} A_j(\sigma_1)^{\nu_j} \right) = E(\sigma_1) X(\sigma_1). \quad (18)$$

Due to its length and technical nature we have given the proof of this lemma in the appendix.

3.3 The output matrix, $C(\sigma_1)$

The output matrix is related with the image of the $q \times q$ identity matrix under the canonical map $\mathcal{A}^q \rightarrow \mathcal{M}$. We elaborate on this now. Let s_i denote the i th standard basis (row-)vector for \mathcal{A}^q , and $\overline{s_i}$ its image under the canonical map $\mathcal{A}^q \rightarrow \mathcal{M}$. Now, consider again the map $\psi : \mathcal{A}_d^r \rightarrow \mathcal{M}$ given by equation (9). Since ψ is surjective, for each $s_i \in \mathcal{A}^q$, with $1 \leq i \leq q$, there exists $c_i(\sigma_1) \in \mathcal{A}_d^r$ such that

$$\psi(c_i(\sigma_1)) = \overline{s_i}.$$

The *output matrix* $C(\sigma_1) \in \mathcal{A}_d^{q \times r}$ is obtained by stacking these $c_i(\sigma_1)$'s one below the other. That is,

$$C(\sigma_1) := \begin{bmatrix} c_1(\sigma_1) \\ c_2(\sigma_1) \\ \vdots \\ c_q(\sigma_1) \end{bmatrix} \in \mathcal{A}_d^{q \times r}. \quad (19)$$

3.4 The first order equation

The key observation to obtaining a representation formula for strongly relevant systems (that is, \mathcal{M} being finitely generated over \mathcal{A}_d) is the fact that such systems admit a first order representation. This fact is very much akin to the well-known notion of state space in 1D systems theory. However, unlike 1D systems, the state space in this case is often *not* a finite dimensional vector space. In this subsection, we show the construction of the state space and the corresponding first order representation of the original system, using the three type of matrices introduced in Subsections 3.1, 3.2 and 3.3.

Recall that for strongly relevant systems, the quotient module \mathcal{M} is a finitely generated \mathcal{A}_d -module. This means we have a matrix of relations $X(\sigma_1)$, the companion matrices $A_1(\sigma_1), A_2(\sigma_1), \dots, A_{n-d}(\sigma_1)$, and the output matrix $C(\sigma_1)$. Define the following d -D behavior

$$\mathcal{X} := \left\{ x \in \left(\mathbb{R}^{\mathbb{Z}^d} \right)^r \mid X(\sigma_1)x = 0 \right\}.$$

We call \mathcal{X} the *state space*.

Now note that, as a consequence of statement 4 of Lemma 4, we have, for all $1 \leq j \leq (n-d)$

$$A_i(\sigma_1)\mathcal{X} \subseteq \mathcal{X}. \quad (20)$$

That is, \mathcal{X} is invariant under the action of each of the companion matrices $\{A_i(\sigma_1)\}_{i=1,2,\dots,n-d}$. Therefore, each $A_i(\sigma_1)$ can be thought as an *endomorphism* of \mathcal{X} . We are going to use these companion matrices to define a first order $(n-d)$ -D system over \mathcal{X} . For this purpose, let us denote by \mathbf{x} an $(n-d)$ -D trajectory over \mathcal{X} . Alternatively, \mathbf{x} is a map from $\mathbb{Z}^{n-d} \rightarrow \mathcal{X}$. We now describe the first order system over \mathcal{X} as given below: for $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$,

$$\begin{aligned} \mathbf{x}(\nu_1 + 1, \nu_2, \dots, \nu_{n-d}) &= A_1(\sigma_1)\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) \\ \mathbf{x}(\nu_1, \nu_2 + 1, \dots, \nu_{n-d}) &= A_2(\sigma_1)\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) \\ &\vdots \\ \mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d} + 1) &= A_{n-d}(\sigma_1)\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}). \end{aligned}$$

Remark 5. Note that \mathbf{x} can also be identified as an n -D trajectory. This identification is done as follows. Suppose $\nu = (\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$ is arbitrary. Then \mathbf{x} , identified as an n -D trajectory, maps this ν to $(\mathbf{x}(\nu_{d+1}, \nu_{d+2}, \dots, \nu_n))(\nu_1, \nu_2, \dots, \nu_d)$. In what follows we do this identification implicitly throughout the rest of the paper.

With the identification mentioned in Remark 5, it follows that $C(\sigma_1)\mathbf{x}$ can be viewed as an element of $(\mathbb{R}^{\mathbb{Z}^n})^q$. We summarize these constructions in Table 1 below.

TABLE 1	
$\mathcal{X} := \left\{ x \in \left(\mathbb{R}^{\mathbb{Z}^d} \right)^r \mid X(\sigma_1)x = 0 \right\}.$	
$\mathbf{x} : \mathbb{Z}^{n-d} \rightarrow \mathcal{X}.$	
For $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$,	
$\mathbf{x}(\nu_1 + 1, \nu_2, \dots, \nu_{n-d})$	$= A_1(\sigma_1)\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d})$
$\mathbf{x}(\nu_1, \nu_2 + 1, \dots, \nu_{n-d})$	$= A_2(\sigma_1)\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d})$
\vdots	
$\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d} + 1)$	$= A_{n-d}(\sigma_1)\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}).$
$w = C(\sigma_1)\mathbf{x}.$	

With this first order system of equations we are now in a position to state and prove the representation theorem for the strongly relevant systems of order d .

Theorem 6. Suppose $\mathfrak{B} \in \mathfrak{L}^q$ is a strongly relevant autonomous system of order d . That is, the quotient module \mathcal{M} of \mathfrak{B} is finitely generated as a module over \mathcal{A}_d . Then there exist a positive integer r and the following matrices:

- $X(\sigma_1) \in \mathcal{A}_d^{\bullet \times r}$,
- $A_1(\sigma_1), A_2(\sigma_1), \dots, A_{n-d}(\sigma_1) \in \mathcal{A}_d^{r \times r}$,
- $C(\sigma_1) \in \mathcal{A}_d^{q \times r}$,

such that \mathfrak{B} admits the following representation:

$$\mathfrak{B} = \left\{ w \in \left(\mathbb{R}^{\mathbb{Z}^n} \right)^q \mid \exists \mathbf{x} \in \left(\mathbb{R}^{\mathbb{Z}^n} \right)^r \text{ such that equations in Table 1 are satisfied} \right\} \quad (21)$$

We need the following lemma to prove Theorem 6. The lemma concerns a test, involving the matrices $X(\boldsymbol{\sigma}_1), A_1(\boldsymbol{\sigma}_1), \dots, A_{n-d}(\boldsymbol{\sigma}_1), C(\boldsymbol{\sigma}_1)$, as to whether a given vector $r(\boldsymbol{\sigma}) \in \mathcal{A}^q$ maps to 0 under the canonical surjection $\mathcal{A}^q \rightarrow \mathcal{M}$.

Lemma 7. *Let $\mathcal{M} = \mathcal{A}^q/\mathcal{R}$ be a finitely generated module over \mathcal{A}_d with $\{g_1, \dots, g_r\}$ as a generating set. Let $\psi : \mathcal{A}_d^r \rightarrow \mathcal{M}$ be given by equation (9) and let $X(\boldsymbol{\sigma}_1) \in \mathcal{A}_d^{k \times r}$ be a matrix of relations of $\{g_1, \dots, g_r\}$. Further, for $1 \leq j \leq (n-d)$, let $A_j(\boldsymbol{\sigma}_1)$ be as defined by equation (13), and let $C(\boldsymbol{\sigma}_1) \in \mathcal{A}_d^{q \times r}$ be as defined in equation (19). Suppose $f(\boldsymbol{\sigma}) \in \mathcal{A}^q$ is given by*

$$f(\boldsymbol{\sigma}) = \sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \boldsymbol{\sigma}^\nu$$

with $\alpha_\nu \in \mathbb{R}_{\text{row}}^q$ and only finitely many of $\{\alpha_\nu\}$ nonzero. Then the following statements are equivalent:

1. $f(\boldsymbol{\sigma}) \in \mathcal{R}$.
2. $\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\boldsymbol{\sigma}_1) \prod_{j=1}^{n-d} A_j(\boldsymbol{\sigma}_1)^{\nu_{d+j}} \in \ker(\psi)$.
3. There exists a matrix $F(\boldsymbol{\sigma}_1) \in \mathcal{A}_d^{q \times k}$ such that

$$\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\boldsymbol{\sigma}_1) \prod_{j=1}^{n-d} A_j(\boldsymbol{\sigma}_1)^{\nu_{d+j}} = F(\boldsymbol{\sigma}_1) X(\boldsymbol{\sigma}_1).$$

Proof : The proof follows by noting how a typical element, say $f(\boldsymbol{\sigma}) \in \mathcal{A}^q$, corresponds to a vector in \mathcal{A}_d^r , such that the images of these two elements under the maps $\mathcal{A}^q \rightarrow \mathcal{M}$ and $\psi : \mathcal{A}_d^r \rightarrow \mathcal{M}$, respectively, coincide with each other. That is, given $f(\boldsymbol{\sigma}) \in \mathcal{A}^q$, how we can find out an $r(\boldsymbol{\sigma}_1) \in \mathcal{A}_d^r$ such that

$$\psi(r(\boldsymbol{\sigma}_1)) = \overline{f(\boldsymbol{\sigma})}.$$

To get this correspondence, first consider $f(\boldsymbol{\sigma})$ to be a monomial, that is, $f(\boldsymbol{\sigma}) = \alpha \boldsymbol{\sigma}^\nu$, where $\alpha \in \mathbb{R}_{\text{row}}^q$ and $\nu \in \mathbb{Z}^n$. In this case, the image of $f(\boldsymbol{\sigma})$ under the canonical map $\mathcal{A}^q \rightarrow \mathcal{M}$ is given by

$$\overline{f(\boldsymbol{\sigma})} = \alpha \overline{\boldsymbol{\sigma}^\nu}. \quad (22)$$

Let us denote the i^{th} component ν by ν_i . Then by partitioning $\boldsymbol{\sigma}$ into $\boldsymbol{\sigma}_1$ and $\boldsymbol{\sigma}_2$ we can rewrite equation (22) as

$$\begin{aligned} \overline{f(\boldsymbol{\sigma})} &= \overline{\alpha \boldsymbol{\sigma}^\nu} \\ &= \overline{\alpha} \prod_{i=1}^d \overline{\sigma_i^{\nu_i}} \prod_{i=d+1}^n \overline{\sigma_i^{\nu_i}} \\ &= \overline{\alpha \boldsymbol{\sigma}_1^{\nu_1}} \prod_{i=d+1}^n \overline{\sigma_i^{\nu_i}}, \end{aligned} \quad (23)$$

where $\boldsymbol{\nu}_1$ denotes $(\nu_1, \nu_2, \dots, \nu_d)$. Now note that for $\alpha \in \mathbb{R}_{\text{row}}^q$, it follows from the definition of the output matrix $C(\boldsymbol{\sigma}_1)$ that

$$\overline{\alpha} = \psi(\alpha C(\boldsymbol{\sigma}_1)).$$

Therefore, since ψ is an \mathcal{A}_d -module morphism, we also get

$$\overline{\alpha \boldsymbol{\sigma}_1^{\nu_1}} = \psi(\alpha \boldsymbol{\sigma}_1^{\nu_1} C(\boldsymbol{\sigma}_1)).$$

Putting this in equation (23) we get

$$\begin{aligned}
\overline{f(\boldsymbol{\sigma})} &= \overline{\alpha \boldsymbol{\sigma}_1}^{\nu_1} \prod_{i=d+1}^n \overline{\sigma_i}^{\nu_i} \\
&= \psi(\alpha \boldsymbol{\sigma}_1^{\nu_1} C(\boldsymbol{\sigma}_1)) \prod_{i=d+1}^n \overline{\sigma_i}^{\nu_i} \\
&= (\mu_1^{\nu_{d+1}} \circ \mu_2^{\nu_{d+2}} \circ \dots \circ \mu_{n-d}^{\nu_n}) \psi(\alpha \boldsymbol{\sigma}_1^{\nu_1} C(\boldsymbol{\sigma}_1)) \\
&= \psi \left(\alpha \boldsymbol{\sigma}_1^{\nu_1} C(\boldsymbol{\sigma}_1) \prod_{i=1}^{n-d} A_i(\boldsymbol{\sigma}_1)^{\nu_{d+i}} \right),
\end{aligned}$$

where the last equality follows from statement 3 of Lemma 4.

For the case when $f(\boldsymbol{\sigma}) \in \mathcal{A}^q$ has more than one terms, we note that ψ is \mathcal{A}_d -linear. Therefore, the above argument can be applied term-wise. Thus, for an $f(\boldsymbol{\sigma}) \in \mathcal{A}^q$ given by

$$f(\boldsymbol{\sigma}) = \sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \boldsymbol{\sigma}^\nu$$

we get

$$\overline{f(\boldsymbol{\sigma})} = \psi \left(\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\boldsymbol{\sigma}_1) \prod_{j=1}^{n-d} A_j(\boldsymbol{\sigma}_1)^{\nu_{d+j}} \right) \quad (24)$$

The result of the lemma then easily follows by noting that $f(\boldsymbol{\sigma}) \in \mathcal{R}$ if and only if $\overline{f(\boldsymbol{\sigma})} = 0 \in \mathcal{M}$. \square

With Lemma 7 we are now in a position to prove Theorem 6.

Proof of Theorem 6: Suppose $\mathfrak{B} \in \mathcal{L}^q$ is an autonomous behavior with quotient module \mathcal{M} . Let us define $\mathfrak{B}_{\text{aux}}$ as the set of trajectories admitting the representation given by Table 1. That is,

$$\mathfrak{B}_{\text{aux}} := \left\{ w \in \left(\mathbb{R}^{\mathbb{Z}^n} \right)^q \mid \exists \mathbf{x} \in \left(\mathbb{R}^{\mathbb{Z}^n} \right)^r \text{ such that equations in Table 1 are satisfied} \right\}. \quad (25)$$

Then we have to show the following equality of two sets of trajectories:

$$\mathfrak{B} = \mathfrak{B}_{\text{aux}}.$$

(To show $\mathfrak{B} \subseteq \mathfrak{B}_{\text{aux}}$) We have to show that $w \in \mathfrak{B}$ implies that there exists $\mathbf{x} \in \left(\mathbb{R}^{\mathbb{Z}^n} \right)^r$ such that equations in Table 1 are satisfied. For the sake of easy referencing we reproduce the equations given in Table 1: for all $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$, \mathbf{x} satisfies

$$\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathcal{X}, \text{ and} \quad (26)$$

$$\left. \begin{aligned}
\mathbf{x}(\nu_1 + 1, \nu_2, \dots, \nu_{n-d}) &= A_1(\boldsymbol{\sigma}_1) \mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) \\
\mathbf{x}(\nu_1, \nu_2 + 1, \dots, \nu_{n-d}) &= A_2(\boldsymbol{\sigma}_1) \mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) \\
&\vdots \\
\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d} + 1) &= A_{n-d}(\boldsymbol{\sigma}_1) \mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}),
\end{aligned} \right\} \quad (27)$$

with

$$w = C(\boldsymbol{\sigma}_1) \mathbf{x}. \quad (28)$$

In order to get this \mathbf{x} suppose $\{g_1, g_2, \dots, g_r\} \subseteq \mathcal{M}$ is a generating set for \mathcal{M} as a module over \mathcal{A}_d . Now, let us define for $w \in \mathfrak{B}$ the following r -tuple of n -D trajectories:

$$\mathbf{x} := \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} w. \quad (29)$$

We claim that the \mathbf{x} defined above satisfies equations (26), (27) and (28).

We first show that $\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathcal{X}$ for all $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$. Note that it follows from the defining equation (29) of \mathbf{x} that

$$\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} w(\bullet, \nu_1, \nu_2, \dots, \nu_{n-d}).$$

We make the matrix of relations $X(\sigma_1)$ act on $\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d})$ to get

$$\begin{aligned} X(\sigma_1)\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) &= X(\sigma_1) \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} w(\bullet, \nu_1, \nu_2, \dots, \nu_{n-d}) \\ &= \overline{X(\sigma_1)} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} w(\bullet, \nu_1, \nu_2, \dots, \nu_{n-d}) \\ &= \psi(X(\sigma_1)) w(\bullet, \nu_1, \nu_2, \dots, \nu_{n-d}) \\ &= 0, \end{aligned}$$

because $\text{rowspan}(X(\sigma_1)) = \ker(\psi)$. Therefore, \mathbf{x} satisfies equation (26).

We now show that \mathbf{x} satisfies the system of equations (27). Let $i \in \{1, 2, \dots, (n-d)\}$ and $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$ be arbitrary. Recall how \mathbf{x} is treated as an element in $(\mathbb{R}^{\mathbb{Z}^n})^r$; see Remark 5. Under this identification, it follows that

$$\mathbf{x}(\nu_1, \nu_2, \dots, \nu_i + 1, \dots, \nu_{n-d}) = \sigma_{d+i}\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}). \quad (30)$$

Applying the defining equation (29) of \mathbf{x} to equation (30) above we get

$$\begin{aligned} \mathbf{x}(\nu_1, \nu_2, \dots, \nu_i + 1, \dots, \nu_{n-d}) &= \sigma_{d+i}\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) \\ &= \sigma_{d+i} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} w(\bullet, \nu_1, \nu_2, \dots, \nu_{n-d}) \\ &= \overline{\sigma_{d+i}} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} w(\bullet, \nu_1, \nu_2, \dots, \nu_{n-d}) \\ &= \mu_i \left(\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} \right) w(\bullet, \nu_1, \nu_2, \dots, \nu_{n-d}) \\ &= A_i(\sigma_1) \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} w(\bullet, \nu_1, \nu_2, \dots, \nu_{n-d}), \end{aligned}$$

where the last equation follows from equation (14). Therefore, we get

$$\mathbf{x}(\nu_1, \nu_2, \dots, \nu_i + 1, \dots, \nu_{n-d}) = A_i(\boldsymbol{\sigma}_1) \mathbf{x}(\nu_1, \nu_2, \dots, \nu_i, \dots, \nu_{n-d})$$

for all $1 \leq i \leq (n-s)$ and $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$. That is, \mathbf{x} satisfies equation (27).

Finally, we have to show that \mathbf{x} and w satisfy equation (28). This follows from the definition of the output matrix $C(\boldsymbol{\sigma}_1)$. Multiplying both sides of equation (29) by $C(\boldsymbol{\sigma}_1)$ we get

$$\begin{aligned} C(\boldsymbol{\sigma}_1) \mathbf{x} &= C(\boldsymbol{\sigma}_1) \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{bmatrix} w \\ &= \psi(C(\boldsymbol{\sigma}_1)) w = \overline{I}_q w = w. \end{aligned}$$

This concludes the $\mathfrak{B} \subseteq \mathfrak{B}_{\text{aux}}$.

(To show $\mathfrak{B} \supseteq \mathfrak{B}_{\text{aux}}$) We now show that if we obtain a w by solving the system of equations in Table 1, that is, equations (26), (27), (28), then that w is in \mathfrak{B} . Let $\mathcal{R} \subseteq \mathcal{A}^q$ be the equation module of \mathfrak{B} . Then, it is enough to show that the action of every element $r(\boldsymbol{\sigma}) \in \mathcal{R}$ on any $w \in \mathfrak{B}_{\text{aux}}$ produces the zero trajectory.

Now, let $r(\boldsymbol{\sigma})$ be any element in \mathcal{R} given in an expanded form as

$$r(\boldsymbol{\sigma}) = \sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \boldsymbol{\sigma}^\nu,$$

where $\alpha_\nu \in \mathbb{R}_{\text{row}}^q$ and all of them but finitely many are zero. Once again, we partition the shift operators into two, namely $\{\sigma_1, \dots, \sigma_d\}$ and $\{\sigma_{d+1}, \dots, \sigma_n\}$, to rewrite $r(\boldsymbol{\sigma})$ as

$$r(\boldsymbol{\sigma}) = \sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} \prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_{d+i}},$$

where $(\nu_1, \nu_2, \dots, \nu_n) = \nu$. Then, this $r(\boldsymbol{\sigma})$ is made to act upon an arbitrary $w \in \mathfrak{B}_{\text{aux}}$ to get the following:

$$\begin{aligned} r(\boldsymbol{\sigma}) w &= \left(\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} \prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_{d+i}} \right) w \\ &= \left(\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} \prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_{d+i}} \right) C(\boldsymbol{\sigma}_1) \mathbf{x} \\ &= \left(\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\boldsymbol{\sigma}_1) \prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_{d+i}} \right) \mathbf{x} \\ &= \left(\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\boldsymbol{\sigma}_1) \left(\prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_{d+i}} \mathbf{x} \right) \right). \end{aligned} \tag{31}$$

Before proceeding, note that

$$\sigma_{d+i}^{\nu_{d+i}} \mathbf{x} = A_i(\boldsymbol{\sigma}_1)^{\nu_{d+i}} \mathbf{x},$$

because \mathbf{x} satisfies the first order system equations (27). Putting this in equation (31) above we get

$$\begin{aligned} r(\boldsymbol{\sigma}) w &= \left(\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\boldsymbol{\sigma}_1) \left(\prod_{i=1}^{n-d} A_i(\boldsymbol{\sigma}_1)^{\nu_{d+i}} \mathbf{x} \right) \right) \\ &= \left(\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\boldsymbol{\sigma}_1) \prod_{i=1}^{n-d} A_i(\boldsymbol{\sigma}_1)^{\nu_{d+i}} \right) \mathbf{x}. \end{aligned} \tag{32}$$

Since $r(\sigma) \in \mathcal{R}$, by Lemma 7, there exists $F(\sigma_1) \in \mathcal{A}_d^{q \times k}$ such that

$$\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\sigma_1) \prod_{i=1}^{n-d} A_i(\sigma_1)^{\nu_{d+i}} = F(\sigma_1) X(\sigma_1).$$

Making use of this observation in equation (32) above we get that

$$\begin{aligned} r(\sigma)w &= \left(\sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \prod_{i=1}^d \sigma_i^{\nu_i} C(\sigma_1) \prod_{i=1}^{n-d} A_i(\sigma_1)^{\nu_{d+i}} \right) \mathbf{x} \\ &= F(\sigma_1) X(\sigma_1) \mathbf{x} = 0, \end{aligned}$$

where the last equation follows from the fact that \mathbf{x} satisfies equation (26), that is,

$$\mathbf{x}(\nu_1, \dots, \nu_{n-d}) \in \mathcal{X} = \ker(X(\sigma_1))$$

for all $(\nu_1, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$. Therefore, $w \in \mathfrak{B}$, and this concludes the $\mathfrak{B} \supseteq \mathfrak{B}_{\text{aux}}$ part of the proof. \square

We illustrate this result in the following example.

Example 8. Let us consider the 3-D scalar system given by the following kernel representation:

$$\mathfrak{B} = \ker \begin{bmatrix} \sigma_3^2 - 2\sigma_3 + 1 \\ \sigma_2^2 - 2\sigma_2 + 1 \\ \sigma_1\sigma_3 - \sigma_1 - \sigma_2 - \sigma_3 + 2 \end{bmatrix}.$$

In this case, clearly, $\mathcal{A} = \mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}, \sigma_3, \sigma_3^{-1}]$. The role of the equation module \mathcal{R} is played by the ideal $\mathfrak{a} = \langle \sigma_3^2 - 2\sigma_3 + 1, \sigma_2^2 - 2\sigma_2 + 1, \sigma_1\sigma_3 - \sigma_1 - \sigma_2 - \sigma_3 + 2 \rangle$. It can be checked that the quotient ring $\mathcal{M} = \mathcal{A}/\mathfrak{a}$ is finitely generated as a module over $\mathcal{A}_1 = \mathbb{R}[\sigma_1, \sigma_1^{-1}]$. Therefore, \mathfrak{B} is strongly relevant of order 1. Let us compute the required matrices. As in the main text, let $A_1(\sigma_1), A_2(\sigma_2)$ represent multiplications by σ_1, σ_2 , respectively, in \mathcal{M} . First, we need to fix a generating set for \mathcal{A}/\mathfrak{a} as a module over \mathcal{A}_1 . The set $\{\bar{1}, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_2\bar{\sigma}_3\}$ meets the requirement for an appropriate generating set. The matrices $A_1(\sigma_1)$ and $A_2(\sigma_1)$, in this case, are given by

$$A_1(\sigma_1) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 2 \end{bmatrix}, \quad A_2(\sigma_1) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 2 & 0 \\ 0 & -1 & 0 & 2 \end{bmatrix}.$$

Note that both $A_1(\sigma_1)$ and $A_2(\sigma_1)$ are invertible over \mathcal{A}_1 . A matrix of relations, $X(\sigma_1)$, for the chosen generating set is given by

$$X(\sigma_1) = \begin{bmatrix} 1 & -1 & -1 & 1 \\ -\sigma_1 + 2 & -1 & \sigma_1 - 1 & 0 \end{bmatrix}.$$

It is easily checked that statements 3 and 4 of Lemma 4 are satisfied here, that is,

$$X(\sigma_1)A_1(\sigma_1) = \begin{bmatrix} 1 & 0 \\ \sigma_1 - 1 & 1 \end{bmatrix} X(\sigma_1), \quad X(\sigma_1)A_2(\sigma_1) = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} X(\sigma_1).$$

The state space \mathcal{X} is thus given by

$$\mathcal{X} = \ker X(\sigma_1) \subseteq \left(\mathbb{R}^{\mathbb{Z}}\right)^4.$$

The output matrix $C(\sigma_1)$ turns out to be

$$C(\sigma_1) = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}.$$

Now, according to Theorem 6, $w \in \mathfrak{B}$ if and only if there exists $\mathbf{x} : \mathbb{Z}^2 \rightarrow \mathcal{X}$ such that

$$\begin{cases} \mathbf{x}(\nu_1 + 1, \nu_2) &= A_1(\sigma_1)\mathbf{x}(\nu_1, \nu_2) \\ \mathbf{x}(\nu_1, \nu_2 + 1) &= A_2(\sigma_1)\mathbf{x}(\nu_1, \nu_2), \end{cases} \quad (33)$$

and $w = C(\sigma_1)\mathbf{x}$.

Remark 9. It is interesting to note that in Example 8, by utilizing the first order representation, an explicit solution formula for $w \in \mathfrak{B}$ can be given. Note that every $\mathbf{x} : \mathbb{Z}^2 \rightarrow \mathcal{X}$ satisfying equation (33) can be obtained as

$$\mathbf{x}(\nu_1, \nu_2) = A_1(\sigma_1)^{\nu_1} A_2(\sigma_1)^{\nu_2} x,$$

where $x \in (\mathbb{R}^{\mathbb{Z}})^4$ satisfies $X(\sigma_1)x = 0$, that is, $x \in \mathcal{X}$. Now note that $w = C(\sigma_1)\mathbf{x}$. Therefore, by the identification as per Remark 5,

$$w(\nu_1, \nu_2, \nu_3) = (C(\sigma_1)\mathbf{x}(\nu_2, \nu_3))(\nu_1).$$

With this, now we can make use of the explicit solution formula for \mathbf{x} to obtain a similar solution formula for w . This is given by

$$w(\nu_1, \nu_2, \nu_3) = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 2 \end{bmatrix}^{\nu_2} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 2 & 0 \\ 0 & -1 & 0 & 2 \end{bmatrix}^{\nu_3} x(\nu_1) \quad (34)$$

We utilize this solution formula of equation (34) in Algorithm 11 below.

As a corollary to Theorem 6 we get an equivalent latent-variable representation for every strongly relevant autonomous system of order d .

Corollary 10. *Let $\mathfrak{B} \in \mathfrak{L}^q$ be an autonomous system that is strongly relevant of order d . Then there exist*

- a positive integer r ,
- a matrix $X(\sigma_1) \in \mathcal{A}_d^{\bullet \times r}$,
- a set of $n - d$ square matrices $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1) \in \mathcal{A}_d^{r \times r}$,
- a matrix $C(\sigma_1) \in \mathcal{A}_d^{q \times r}$

such that \mathfrak{B} admits the following latent variable representation:

$$\mathfrak{B} = \left\{ w \in (\mathbb{R}^{\mathbb{Z}^n})^q \mid \exists \mathbf{x} \in (\mathbb{R}^{\mathbb{Z}^n})^r \text{ satisfying } \begin{bmatrix} X(\sigma_1) & \vdots & 0 \\ \sigma_{d+1}I_r - A_1(\sigma_1) & \vdots & 0 \\ \sigma_{d+2}I_r - A_2(\sigma_1) & \vdots & 0 \\ \vdots & \vdots & \vdots \\ \sigma_n I_r - A_{n-d}(\sigma_1) & \vdots & 0 \\ -C(\sigma_1) & \vdots & I_q \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ w \end{bmatrix} = 0 \right\} \quad (35)$$

3.5 An algorithm for obtaining all solutions

Theorem 6 provides a useful algorithm for obtaining all solutions to a strongly relevant autonomous system. We describe this algorithm now. The algorithm involves two steps, which we call *regularization* and *recursion*.

Given a strongly relevant autonomous system of order d , we first obtain the matrices $X(\sigma_1)$, $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1)$, and $C(\sigma_1)$. We call this process the *regularization* step. This step requires finding out a suitable set of generators for the finitely generated \mathcal{A}_d -module \mathcal{M} . One has to be careful in choosing the generating set so as to ensure that the companion matrices $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1)$ are all invertible over \mathcal{A}_d . This can be implemented on a computer by standard computer algebra packages. In this paper, we do not go into the details of issues related to such an implementation.

The regularization step leads to the *recursion* step, where the companion matrices are used recursively on trajectories in $\mathcal{X} = \ker(X(\sigma_1))$ to obtain solutions to the original system. The recursion indeed gives the solutions because of the first order system equations listed in Table 1.

In order to see that the recursion gives an explicit solution formula for trajectories in the original system, first note that solutions to the first order system defined on \mathcal{X} by equations given in Table 1 can be written explicitly as follows:

$$\mathbf{x}(\nu_1, \nu_2, \dots, \nu_{n-d}) = \prod_{i=1}^{n-d} A_i(\sigma_1)^{\nu_i} x, \quad (36)$$

for arbitrary $(\nu_1, \nu_2, \dots, \nu_{n-d}) \in \mathbb{Z}^{n-d}$, where $x \in (\mathbb{R}^{\mathbb{Z}^d})^r$ satisfies $X(\sigma_1)x = 0$. Since $w = C(\sigma_1)\mathbf{x}$, recalling the identification of \mathbf{x} as a trajectory in $(\mathbb{R}^{\mathbb{Z}^n})^q$ we get

$$w(\nu_1, \nu_2, \dots, \nu_n) = (C(\sigma_1)\mathbf{x}(\nu_{d+1}, \nu_{d+2}, \dots, \nu_n))(\nu_1, \nu_2, \dots, \nu_d),$$

for $(\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$. Utilizing equation (36) now we get

$$w(\nu_1, \nu_2, \dots, \nu_n) = \left(C(\sigma_1) \prod_{i=1}^{n-d} A_i(\sigma_1)^{\nu_{d+i}} x \right) (\nu_1, \nu_2, \dots, \nu_d). \quad (37)$$

Algorithm 11 below elaborates how this equation (37) can be used to obtain *all* solutions to a given strongly relevant autonomous system.

Algorithm 11. (Solution formula for strongly relevant systems of order d)

Regularization	
Input:	An autonomous system $\mathfrak{B} = \ker(R(\sigma))$, where $R(\sigma) \in \mathcal{A}^{\bullet \times q}$.
Computation:	Obtain a generating set $\mathcal{G} := \{g_1, \dots, g_r\} \subseteq \mathcal{M}$. Obtain the matrix of relations $X(\sigma_1) \in \mathcal{A}_d^{k \times r}$. Obtain the companion matrices $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1) \in \mathcal{A}_d^{r \times r}$ (ensure that these matrices are invertible in \mathcal{A}_d). Obtain the output matrix $C(\sigma_1) \in \mathcal{A}_d^{q \times r}$.
Output:	The matrices $X(\sigma_1)$, $A_1(\sigma_1)$, \dots , $A_{n-d}(\sigma_1)$, and $C(\sigma_1)$.
Construction of \mathcal{X}	
Input:	The matrix $X(\sigma_1)$.
Computation:	Solve $X(\sigma_1)x = 0$ for $x \in \left(\mathbb{R}^{\mathbb{Z}^d}\right)^r$.
Output:	The set $\mathcal{X} = \{x \in \left(\mathbb{R}^{\mathbb{Z}^d}\right)^r \mid X(\sigma_1)x = 0\}$.
Recursion	
Input:	An $x \in \mathcal{X}$, and the matrices $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1)$, and $C(\sigma_1)$.
Computation:	for $\nu = (\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$ set $w(\nu) = \left(C(\sigma_1) \prod_{i=1}^{n-d} A_i(\sigma_1)^{\nu_{d+i}} x\right) (\nu_1, \nu_2, \dots, \nu_d).$
Output:	The sequence $w := \{w(\nu)\}_{\nu \in \mathbb{Z}^n}$.

Remark 12. From the algorithm above, it makes sense to call the d -D trajectories $x \in \mathcal{X}$ as *initial conditions*. Indeed, the companion matrices act on x as a $(n-d)$ -D *flow operator* to produce all the solutions in the original n -D system \mathfrak{B} . We call this condition that $x \in \mathcal{X}$ that is $X(\sigma_1)x = 0$ as *compatibility condition*. Note that ideally the compatibility condition must be satisfied at every step of the recursion (see Theorem 6). However, it turns out that checking for compatibility only once – at the beginning of the recursion – is enough. This is because the set of trajectories satisfying the compatibility conditions, that is, $\mathcal{X} = \ker(X(\sigma_1))$ is *invariant* under each of the companion matrices $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1)$ (as a consequence of Lemma 4; see equation (20)). This is perhaps the most crucial benefit of the regularization step that it makes the compatibility condition and the recursion independent of each other, plus it ensures that once the compatibility condition is satisfied, it is automatically satisfied in every subsequent step of the recursion.

4 Discrete version of Noether's normalization

There are many autonomous n -D systems that are not strongly relevant. For example, the scalar system $\mathfrak{B} = \ker(\sigma_1\sigma_2 - \sigma_1 - \sigma_2 + 1)$. Here the quotient module is not a finitely generated module over either $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$ or $\mathbb{R}[\sigma_2, \sigma_2^{-1}]$; neither is it a finite dimensional vector space over \mathbb{R} . Therefore, this \mathfrak{B} is not a strongly relevant system of any order. In fact, autonomous systems are more often *not* strongly relevant. For such systems, clearly, the method of solution presented above becomes inapplicable. However, we shall see in this paper that by a normalization process every autonomous system can be rendered to an equivalent strongly relevant system. We call this normalization process the *discrete Noether's normalization lemma (DNNL)*; for it is an analogous version (for Laurent polynomial rings) to the well-known Noether's normalization lemma (for polynomial rings). The result was discovered by E. Noether (1882–1935), who first presented it in her 1926 paper, entitled “Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik p ”, and used it for studying invariant theory of finite groups over fields of arbitrary characteristics. For detailed analysis and applications of this result see [Eis95].

Like the classical Noether's normalization, our DNNL, too, crucially involves a coordinate transformation. However, the space on which we need to do the coordinate transformation differs because we are dealing with Laurent polynomial rings. It turns out that for DNNL we need to do a coordinate transformation on the indexing set \mathbb{Z}^n .

4.1 Coordinate transformations in \mathbb{Z}^n and their effects on \mathcal{A} and \mathcal{A}^q

The idea of change of coordinates and its effects on a behavior are not new (see [Zam98, Val01]), however, we use this idea to a completely new end. By a coordinate change we mean a \mathbb{Z} -linear map from \mathbb{Z}^n to itself of the form

$$\begin{aligned} T : \mathbb{Z}^n &\rightarrow \mathbb{Z}^n \\ \text{col}(\nu_1, \nu_2, \dots, \nu_n) &=: \nu \mapsto T\nu, \end{aligned}$$

where $T \in \mathbb{Z}^{n \times n}$ is a matrix whose determinant is ± 1 . Such matrices are called \mathbb{Z} -unimodular. Note that $\det(T) = \pm 1$ ensures that the columns of T span the whole of \mathbb{Z}^n as a \mathbb{Z} -module. Such a coordinate transformation T induces the following \mathbb{R} -algebra homomorphism from \mathcal{A} to itself.

$$\begin{aligned} \varphi_T : \mathcal{A} &\rightarrow \mathcal{A} \\ \sigma^\nu &\mapsto \sigma^{T\nu} \end{aligned} \tag{38}$$

for all $\nu \in \mathbb{Z}^n$.

Since T is \mathbb{Z} -unimodular, φ_T turns out to be *bijective*; that is, φ_T is an automorphism of the \mathbb{R} -algebra \mathcal{A} . As a consequence, an *ideal* $\mathfrak{a} \subseteq \mathcal{A}$ is mapped to another *ideal* $\varphi_T(\mathfrak{a})$. The map φ_T can be extended to a map from \mathcal{A}^q to itself:

$$\begin{aligned} \widehat{\varphi}_T : \mathcal{A}^q &\rightarrow \mathcal{A}^q \\ [f_1(\sigma) \ f_2(\sigma) \ \cdots \ f_q(\sigma)] &\mapsto [\varphi_T(f_1(\sigma)) \ \varphi_T(f_2(\sigma)) \ \cdots \ \varphi_T(f_q(\sigma))]. \end{aligned} \tag{39}$$

The map $\widehat{\varphi}_T$ is an \mathcal{A} -module morphism via the automorphism φ_T , *i.e.*, for $r(\sigma) \in \mathcal{A}^q$ and $f(\sigma) \in \mathcal{A}$,

$$\widehat{\varphi}_T(f(\sigma)r(\sigma)) = \varphi_T(f(\sigma))\widehat{\varphi}_T(r(\sigma)).$$

The bijective property of φ_T extends to the module case: as a result, $\widehat{\varphi}_T(\mathcal{R})$, the image of a *submodule* $\mathcal{R} \subseteq \mathcal{A}^q$ under $\widehat{\varphi}_T$, too, is a *submodule*.

4.2 Transforming a single polynomial

We start off by normalizing a single polynomial. In Lemma 13 below we show that given any Laurent polynomial f there exists a coordinate transformation matrix T such that the image of f under the corresponding automorphism φ_T has a special structure: $\varphi_T(f)$ is a linear combination of distinct powers of σ_n with all coefficients being units in the smaller ring $\mathcal{A}_{n-1} := \mathbb{R}[\sigma_1, \sigma_1^{-1}, \dots, \sigma_{n-1}, \sigma_{n-1}^{-1}]$. This result is not new; a proof of this result is given in [Par04], where it was used in the context of designing inverse filters for n -D discrete filters. We provide a proof of Lemma 13 here to make this exposition self-contained.

Lemma 13. *Let $f \in \mathcal{A}$ be given by*

$$f = \sum_{\nu \in \mathbb{Z}^n} \alpha_\nu \sigma^\nu, \quad \text{where } \alpha_\nu \in \mathbb{R}, \text{ and only finitely many } \alpha_\nu \neq 0.$$

Then there exists a co-ordinate transformation $T \in \mathbb{Z}^{n \times n}$ such that under the corresponding homomorphism $\varphi_T : \mathcal{A} \rightarrow \mathcal{A}$, we have

$$\varphi_T(f) = \left(\sum_{i=0}^k u_i \sigma_n^i \right) u, \tag{40}$$

where $u_i \in \mathcal{A}_{n-1}$ and $u \in \mathbb{R}[\sigma_n, \sigma_n^{-1}]$ are units and k is some finite positive integer.

Proof : In general, there are many T 's which will render f in the form of equation (40); we construct one particular T for which the monomials of f are mapped to monomials having different σ_n powers. To this end, let us define $T \in \mathbb{Z}^{n \times n}$ as

$$T = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ t_1 & t_2 & \cdots & 1 \end{bmatrix},$$

where $t_1, t_2, \dots, t_{n-1} \in \mathbb{Z}$. Clearly, T is unimodular. The homomorphism φ_T corresponding to this T maps a monomial σ^ν with $\nu = \text{col}(\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$ to the following

$$\varphi_T(\sigma^\nu) = \sigma^{T\nu} = \sigma_1^{\nu_1} \sigma_2^{\nu_2} \cdots \sigma_{n-1}^{\nu_{n-1}} \sigma_n^{t_1\nu_1 + t_2\nu_2 + \cdots + \nu_n}.$$

Let us define $\mathbf{t} := \text{col}(t_1, t_2, \dots, t_{n-1}) \in \mathbb{Z}^{n-1}$, and $\tilde{\mathbf{t}} := \text{col}(\mathbf{t}, 1) \in \mathbb{Z}^n$. Note that the power of σ_n in $\varphi_T(\sigma^\nu)$ is then given by the usual dot product $\langle \tilde{\mathbf{t}}, \nu \rangle$. Let us also define the following finite subset of \mathbb{Z}^n .

$$\text{supp}(f) := \{\nu \in \mathbb{Z}^n \mid \alpha_\nu \neq 0\}.$$

We now claim that \mathbf{t} can be chosen such that the σ_n -degrees of $\varphi_T(\sigma^\nu)$ for $\nu \in \text{supp}(f)$ are all different from each other, *i.e.*, the following set

$$\left\{ \mathbf{t} \in \mathbb{Z}^{n-1} \mid \langle \tilde{\mathbf{t}}, \nu \rangle \neq \langle \tilde{\mathbf{t}}, \nu' \rangle \text{ for all } \nu, \nu' \in \text{supp}(f), \nu \neq \nu' \right\} \neq \emptyset. \quad (41)$$

To verify this claim let us choose two distinct elements from $\text{supp}(f)$, say $\nu = \text{col}(\nu_1, \nu_2, \dots, \nu_n)$ and $\nu' = \text{col}(\nu'_1, \nu'_2, \dots, \nu'_n)$ and consider the following equation

$$\mathbf{t}^T \begin{bmatrix} \nu_1 - \nu'_1 \\ \nu_2 - \nu'_2 \\ \vdots \\ \nu_{n-1} - \nu'_{n-1} \end{bmatrix} = \nu'_n - \nu_n. \quad (42)$$

We consider solutions to this equation (42) with $\mathbf{t} \in \mathbb{R}^{n-1}$, *i.e.*,

$$\mathcal{S}_{\nu, \nu'} = \{ \mathbf{t} \in \mathbb{R}^{n-1} \mid \text{equation (42) is satisfied} \}.$$

The solution set $\mathcal{S}_{\nu, \nu'}$, if nonempty, is an affine hyperplane of dimension $(n-2)$. This follows from the following argument. Since $\nu \neq \nu'$, the vector $\text{col}((\nu_1 - \nu'_1), (\nu_2 - \nu'_2), \dots, (\nu_{n-1} - \nu'_{n-1}))$ and the number $(\nu'_n - \nu_n)$ cannot both be equal to zero simultaneously. Hence, $\mathcal{S}_{\nu, \nu'}$ is either empty or an affine hyperplane of dimension $(n-2)$. Now consider all pairs $\nu, \nu' \in \text{supp}(f)$ and the corresponding $\mathcal{S}_{\nu, \nu'}$'s. Clearly, there are only finitely many such pairs (in fact, their number is $\frac{|\text{supp}(f)|(|\text{supp}(f)|-1)}{2}$). Consider the following union

$$\mathcal{S} := \bigcup_{\nu, \nu' \in \text{supp}(f), \nu \neq \nu'} \mathcal{S}_{\nu, \nu'}.$$

Now observe that the set under consideration in equation (41) is related with the above defined \mathcal{S} as

$$\left\{ \mathbf{t} \in \mathbb{Z}^{n-1} \mid \langle \tilde{\mathbf{t}}, \nu \rangle \neq \langle \tilde{\mathbf{t}}, \nu' \rangle \text{ for all } \nu, \nu' \in \text{supp}(f), \nu \neq \nu' \right\} = (\mathbb{R}^{n-1} \setminus \mathcal{S}) \cap \mathbb{Z}^{n-1}.$$

Since the number of pairs (ν, ν') is finite and each of $\mathcal{S}_{\nu, \nu'}$ is either empty or a hyperplane of dimension $(n-2)$, the union \mathcal{S} cannot contain all of \mathbb{Z}^{n-1} . And therefore, $(\mathbb{R}^{n-1} \setminus \mathcal{S}) \cap \mathbb{Z}^{n-1} \neq \emptyset$, which proves our claim equation (41).

It then follows that we can choose a $\mathbf{t} \in \mathbb{Z}^{n-1}$ such that

$$\langle \tilde{\mathbf{t}}, \nu \rangle \neq \langle \tilde{\mathbf{t}}, \nu' \rangle \text{ for all } \nu, \nu' \in \text{supp}(f), \nu \neq \nu'.$$

In that case, the nonzero monomials appearing in $\varphi_T(f)$ will have all distinct powers of σ_n . Therefore, $\varphi_T(f)$ can be written as

$$\varphi_T(f) = \sum_{\nu \in \text{supp}(f)} \left(\alpha_\nu \prod_{j=1}^{n-1} \sigma_j^{\nu_j} \right) \sigma_n^{\langle \tilde{\mathbf{t}}, \nu \rangle}.$$

Note that $\left(\alpha_\nu \prod_{j=1}^{n-1} \sigma_j^{\nu_j} \right)$ are all units in \mathcal{A}_{n-1} . Rearranged in the ascending order of powers of σ_n we get u_i 's from $\left(\alpha_\nu \prod_{j=1}^{n-1} \sigma_j^{\nu_j} \right)$ s. Further, taking out the smallest power of σ_n and calling it u we get the required expression of equation (40). \square

There is an important consequence of Lemma 13; we state this as Lemma 14 below. This will be essential for the general case Theorem 17, where we deal with normalization of a general (non-principal) ideal.

Lemma 14. *Let $\{0\} \neq \mathfrak{a} \subseteq \mathcal{A}$ be an ideal. Then there exists a coordinate transformation matrix $T \in \mathbb{Z}^{n \times n}$, inducing $\varphi_T : \mathcal{A} \rightarrow \mathcal{A}$, such that*

- $\mathcal{A}/\varphi_T(\mathfrak{a})$ contains $\mathcal{A}_{n-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1})$ as a subring, and
- $\mathcal{A}/\varphi_T(\mathfrak{a})$ is a finitely generated module over $\mathcal{A}_{n-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1})$.

Proof : First note that for an ideal $\mathfrak{a} \subseteq \mathcal{A}$, the quotient ring \mathcal{A}/\mathfrak{a} can be written as

$$\mathcal{A}/\mathfrak{a} = \frac{\mathcal{A}_{n-1}}{\mathfrak{a} \cap \mathcal{A}_{n-1}} [\overline{\sigma_n}, \overline{\sigma_n}^{-1}].$$

This is the algebra generated by $\overline{\sigma_n}$ and $(\overline{\sigma_n})^{-1}$ over $\mathcal{A}_{n-1}/(\mathfrak{a} \cap \mathcal{A}_{n-1})$. As we have already seen, φ_T takes an ideal $\mathfrak{a} \subseteq \mathcal{A}$ to an ideal $\mathfrak{b} = \varphi_T(\mathfrak{a}) \subseteq \mathcal{A}$. Suppose $f \in \mathfrak{a}$ is any nonzero Laurent polynomial. By Lemma 13, there exists a coordinate transformation matrix T such that $\varphi_T(f)$ has the form given by equation (40). Since u in the right-hand-side of equation (40) is a unit in \mathcal{A} , it follows that

$$\varphi_T(f) = \left(\sum_{i=0}^k u_i \sigma_n^i \right) u \in \mathfrak{b} \quad \Leftrightarrow \quad \sum_{i=0}^k u_i \sigma_n^i \in \mathfrak{b}.$$

Further, since $\{u_i\}$ are all units, the coefficient of the highest power of σ_n , i.e. u_k , can be made 1, and the resulting polynomial will still belong to the same ideal. That is,

$$u_k \left(\sigma_n^k + \sum_{i=0}^{k-1} u'_i \sigma_n^i \right) \in \mathfrak{b} \quad \Leftrightarrow \quad \sigma_n^k + \sum_{i=0}^{k-1} u'_i \sigma_n^i \in \mathfrak{b},$$

where $u'_i = u_i u_k^{-1} \in \mathcal{A}_{n-1}$. In other words, $\overline{\sigma_n}$ satisfies a monic polynomial equation in \mathcal{A}/\mathfrak{b} with coefficients coming from $\mathcal{A}_{n-1}/(\mathfrak{b} \cap \mathcal{A}_{n-1})$:

$$(\overline{\sigma_n})^k + \sum_{i=0}^{k-1} \overline{u'_i} (\overline{\sigma_n})^i = 0. \tag{43}$$

Now, suppose we have a Laurent polynomial, say $g \in \mathcal{A}$, which can be written as a polynomial with non-negative powers in σ_n with coefficients from \mathcal{A}_{n-1} . That is, $g \in \mathcal{A}_{n-1}[\sigma_n]$.

Then, we can carry out Euclidean division algorithm by the monic polynomial appearing in equation (43) above to obtain

$$g = \left(\sigma_n^k + \sum_{i=0}^{k-1} u'_i \sigma_n^i \right) q + \sum_{i=0}^{k-1} \alpha_i \sigma_n^i,$$

where $q \in \mathcal{A}_{n-1}[\sigma_n]$ and $\{\alpha_0, \alpha_1, \dots, \alpha_{k-1}\} \subseteq \mathcal{A}_{n-1}$. Equation (43) then implies

$$\bar{g} = \sum_{i=0}^{k-1} \bar{\alpha}_i (\bar{\sigma}_n)^i.$$

Note that the coefficients above are all in $\mathcal{A}_{n-1}/(\mathfrak{b} \cap \mathcal{A}_{n-1})$, and $\bar{g} \in \frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n]$. Thus, every element in $\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n]$ can be written as a finite linear combination of $\{\bar{1}, \bar{\sigma}_n, \dots, (\bar{\sigma}_n)^{k-1}\}$ with coefficients from $\mathcal{A}_{n-1}/(\mathfrak{b} \cap \mathcal{A}_{n-1})$. In other words, $\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n]$ is an $\left(\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}} \right)$ -module generated by $\{\bar{1}, \bar{\sigma}_n, \dots, (\bar{\sigma}_n)^{k-1}\}$.

Further, multiplying both sides of equation (43) by $(\bar{\sigma}_n)^{-1}$ we get

$$(\bar{\sigma}_n)^{k-1} + \sum_{i=1}^{k-1} \bar{u}'_i (\bar{\sigma}_n)^{i-1} + \bar{u}'_0 (\bar{\sigma}_n)^{-1} = 0. \quad (44)$$

Since u'_0 was obtained by multiplying two units, namely u_0 and u_k^{-1} , it follows that \bar{u}'_0 is a unit itself. This is because units in \mathcal{A} go to units in \mathcal{A}/\mathfrak{b} . Therefore equation (44) can be rewritten as

$$(\bar{\sigma}_n)^{-1} = -(\bar{u}'_0)^{-1} (\bar{\sigma}_n)^{k-1} - \sum_{i=1}^{k-1} (\bar{u}'_0)^{-1} \bar{u}'_i (\bar{\sigma}_n)^{i-1}. \quad (45)$$

By taking positive powers in both sides of equation (45), we get that for every $i \in \mathbb{N}$, the monomial $(\bar{\sigma}_n)^{-i}$ can be written as a polynomial in $\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n]$. Therefore, every polynomial in $\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n^{-1}]$ too can be written as a polynomial in $\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n]$. In other words,

$$\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n^{-1}] = \frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n].$$

Hence

$$\mathcal{A}/\mathfrak{b} = \frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n, \bar{\sigma}_n^{-1}] = \frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n]. \quad (46)$$

We have already shown that $\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}}[\bar{\sigma}_n]$ is a finitely generated $\left(\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}} \right)$ -module. Therefore, by equation (46) above, we get that \mathcal{A}/\mathfrak{b} too is a finitely generated $\left(\frac{\mathcal{A}_{n-1}}{\mathfrak{b} \cap \mathcal{A}_{n-1}} \right)$ -module. Also note that \mathcal{A}/\mathfrak{b} contains $\mathcal{A}_{n-1}/(\mathfrak{b} \cap \mathcal{A}_{n-1})$ as a subring. This completes the proof. \square

Remark 15. In the situation of Lemma 14, it follows that every element in $\mathcal{A}/\varphi_T(\mathfrak{a})$ satisfies a *monic polynomial* equation over the subring $\mathcal{A}_{n-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1})$ (see [AM69, Proposition 5.1]). In this case $\mathcal{A}/\varphi_T(\mathfrak{a})$ is said to be an *integral extension* over the subring $\mathcal{A}_{n-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1})$, or equivalently, the map $\mathcal{A}_{n-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1}) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$ is *injective and integral*. The converse of this, that is injective and integral implying the bigger ring being finitely generated module over the smaller ring, is not true in general. However, if the bigger ring is a finitely generated algebra over the smaller ring, then the converse is also true ([AM69, Corollary 5.2]). In our case, for every $1 \leq d \leq n$ and an arbitrary ideal $\mathfrak{a} \subseteq \mathcal{A}$, the quotient ring \mathcal{A}/\mathfrak{a} is the algebra generated by $\{\bar{\sigma}_{d+1}, (\bar{\sigma}_{d+1})^{-1}, \dots, \bar{\sigma}_n, (\bar{\sigma}_n)^{-1}\}$ over $\mathcal{A}_d/(\mathfrak{a} \cap \mathcal{A}_d)$. Thus, \mathcal{A}/\mathfrak{a} is a finitely generated algebra over $\mathcal{A}_d/(\mathfrak{a} \cap \mathcal{A}_d)$. Therefore, in all the cases that follow from now, the following two statements are equivalent:

1. A ring map $\mathcal{A}_d \rightarrow \mathcal{A}/\mathfrak{a}$ is injective and integral.
2. The bigger ring \mathcal{A}/\mathfrak{a} is a finitely generated faithful module over the smaller ring \mathcal{A}_d .

We use the two situations interchangeably in the sequel.

4.3 The general theorem

Lemma 14 above shows that for a nonzero ideal \mathfrak{a} , there exists a coordinate transformation matrix $T \in \mathbb{Z}^{n \times n}$, such that $\mathcal{A}_{n-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1}) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$ is *injective and integral*. Note that the smaller ring $\mathcal{A}_{n-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1})$ may not be a Laurent polynomial ring because the intersection ideal $\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1}$ may not be the zero ideal. However, it is desirable to have the smaller ring to be a Laurent polynomial ring itself. Theorem 17 shows how this can be done with a suitable coordinate transformation T . We shall require the following Lemma 16 to prove Theorem 17. As done in [KR00] for the conventional Noether's Normalization Lemma, we also follow an induction strategy for the proof of Theorem 17. While Lemma 14 provides the first step of the induction, the inductive step is what Lemma 16 deals with. The lemma tells us that if we already have an injective and integral ring map $\mathcal{A}_d/(\mathfrak{a} \cap \mathcal{A}_d) \rightarrow \mathcal{A}/\mathfrak{a}$ such that $\mathfrak{a} \cap \mathcal{A}_d \neq \{0\}$, then by using a coordinate transformation T we can go down one step further and have $\mathcal{A}_{d-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d-1}) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$ injective and integral.

Lemma 16. *Let $\{0\} \neq \mathfrak{a} \subseteq \mathcal{A}$ be an ideal and $1 \leq d \leq n$ an integer such that $\mathcal{A}_d/(\mathfrak{a} \cap \mathcal{A}_d) \rightarrow \mathcal{A}/\mathfrak{a}$ is injective and integral. Suppose that $\mathfrak{a} \cap \mathcal{A}_d \neq \{0\}$. Then there exists $T \in \mathbb{Z}^{n \times n}$, inducing $\varphi_T : \mathcal{A} \ni \sigma^\nu \mapsto \sigma^{T\nu} \in \mathcal{A}$ for all $\nu \in \mathbb{Z}^n$, such that $\mathcal{A}_{d-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d-1}) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$ is injective and integral.*

Proof : We first define $\tilde{\mathfrak{a}} := \mathfrak{a} \cap \mathcal{A}_d$ an ideal in \mathcal{A}_d , and then apply Lemma 14 to $\tilde{\mathfrak{a}}$ and \mathcal{A}_d . Since $\tilde{\mathfrak{a}} \neq \{0\}$, by Lemma 14, there exists a unimodular $\tilde{T} \in \mathbb{Z}^{d \times d}$ inducing the automorphism $\varphi_{\tilde{T}} : \mathcal{A}_d \rightarrow \mathcal{A}_d$ such that

$$\mathcal{A}_{d-1}/(\varphi_{\tilde{T}}(\tilde{\mathfrak{a}}) \cap \mathcal{A}_{d-1}) \rightarrow \mathcal{A}_d/\varphi_{\tilde{T}}(\tilde{\mathfrak{a}}) \quad (47)$$

is injective and integral.

With this \tilde{T} we now define our desired coordinate transformation on \mathbb{Z}^n as $T := \begin{bmatrix} \tilde{T} & 0 \\ 0 & I_{n-d} \end{bmatrix} \in \mathbb{Z}^{n \times n}$. Note that the restriction of T on the first d coordinate axes is \tilde{T} and that on the rest of the coordinate axes is identity. Therefore, the corresponding $\varphi_T : \mathcal{A} \rightarrow \mathcal{A}$ maps elements from \mathcal{A}_d to itself. In fact, $\varphi_T|_{\mathcal{A}_d} = \varphi_{\tilde{T}}$. Since $\varphi_{\tilde{T}}$ is an automorphism of \mathcal{A}_d , we get that

$$\varphi_T(\mathcal{A}_d) = \varphi_{\tilde{T}}(\mathcal{A}_d) = \mathcal{A}_d. \quad (48)$$

Now, since action of φ_T restricted to \mathcal{A}_d matches that of $\varphi_{\tilde{T}}$ on \mathcal{A}_d we get $\varphi_{\tilde{T}}(\tilde{\mathfrak{a}}) = \varphi_T(\tilde{\mathfrak{a}})$. Note that, since φ_T is a bijection, we have $\varphi_T(\mathfrak{a} \cap \mathcal{A}_d) = \varphi_T(\mathfrak{a}) \cap \varphi_T(\mathcal{A}_d)$. So, we can write

$$\varphi_T(\tilde{\mathfrak{a}}) = \varphi_T(\mathfrak{a}) \cap \varphi_T(\mathcal{A}_d) = \varphi_T(\mathfrak{a}) \cap \mathcal{A}_d \text{ (by equation (48))}.$$

Since $\mathcal{A}_{d-1} \subseteq \mathcal{A}_d$, we get from the above equation

$$\varphi_{\tilde{T}}(\tilde{\mathfrak{a}}) \cap \mathcal{A}_{d-1} = \varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d-1}.$$

Thus equation (47) can be rewritten as:

$$\mathcal{A}_{d-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d-1}) \rightarrow \mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d) \quad (49)$$

is injective and integral.

We now claim that $\mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$ is injective and integral. In order to see this, first note that, like before, $\mathcal{A}/\varphi_T(\mathfrak{a})$ can be written as a finitely generated algebra over the smaller ring $\mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d)$ as

$$\mathcal{A}/\varphi_T(\mathfrak{a}) = \frac{\mathcal{A}_d}{\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d} [\overline{\sigma_{d+1}}, (\overline{\sigma_{d+1}})^{-1}, \dots, \overline{\sigma_n}, (\overline{\sigma_n})^{-1}].$$

So, in order to prove our claim, it is enough to show that each of the generators of the algebra written above is integral over the smaller ring. That is, for all $d+1 \leq i \leq n$, $\overline{\sigma_i}$ and $(\overline{\sigma_i})^{-1}$ satisfy monic polynomial equations over $\mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d)$. Now, by assumption, \mathcal{A}/\mathfrak{a} is integral over $\mathcal{A}_d/(\mathfrak{a} \cap \mathcal{A}_d)$. This means for $d+1 \leq i \leq n$, $\overline{\sigma_i}$ and $(\overline{\sigma_i})^{-1}$ satisfy monic polynomial equations over $\mathcal{A}_d/(\mathfrak{a} \cap \mathcal{A}_d)$. That is, for $d+1 \leq i \leq n$, there exist positive integers k_i and r_i , and $a_{i0}, a_{i1}, \dots, a_{ik_i-1} \in \mathcal{A}_d$ and $b_{i0}, b_{i1}, \dots, b_{ir_i-1} \in \mathcal{A}_d$ such that we have

$$\left. \begin{array}{l} \sigma_i^{k_i} + a_{ik_i-1} \sigma_i^{k_i-1} + \dots + a_{i1} \sigma_i + a_{i0} \in \mathfrak{a} \\ (\sigma_i^{-1})^{r_i} + b_{ir_i-1} (\sigma_i^{-1})^{r_i-1} + \dots + b_{i1} \sigma_i^{-1} + b_{i0} \in \mathfrak{a} \end{array} \right\} \quad (50)$$

We then apply φ_T to equation (50) and use the fact that for $d+1 \leq i \leq n$ we have $\varphi_T(\sigma_i) = \sigma_i$ and $\varphi_T(\sigma_i^{-1}) = \sigma_i^{-1}$. Thus we get

$$\left. \begin{array}{l} \sigma_i^{k_i} + \varphi_T(a_{ik_i-1}) \sigma_i^{k_i-1} + \dots + \varphi_T(a_{i1}) \sigma_i + \varphi_T(a_{i0}) \in \varphi_T(\mathfrak{a}) \\ (\sigma_i^{-1})^{r_i} + \varphi_T(b_{ir_i-1}) (\sigma_i^{-1})^{r_i-1} + \dots + \varphi_T(b_{i1}) \sigma_i^{-1} + \varphi_T(b_{i0}) \in \varphi_T(\mathfrak{a}) \end{array} \right\} \quad (51)$$

As we have already seen, from the definition of φ_T it follows that \mathcal{A}_d is invariant under φ_T , that is, φ_T maps elements from \mathcal{A}_d to itself. Therefore, $\varphi_T(a_{i0}), \varphi_T(a_{i1}), \dots, \varphi_T(a_{ik_i-1}) \in \mathcal{A}_d$ and $\varphi_T(b_{i0}), \varphi_T(b_{i1}), \dots, \varphi_T(b_{ir_i-1}) \in \mathcal{A}_d$. Thus equation (51) shows that for all $d+1 \leq i \leq n$, both $\overline{\sigma_i}, (\overline{\sigma_i})^{-1} \in \mathcal{A}/\varphi_T(\mathfrak{a})$ satisfy monic polynomial equations with coefficients coming from $\mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d)$, which means $\mathcal{A}/\varphi_T(\mathfrak{a})$ is integral over $\mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d)$. That

$$\mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$$

is injective is obvious. Therefore our claim that $\mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$ is injective and integral is true.

By combining equation (49) with this we get the following two-stage tower of integral ring extensions:

$$\mathcal{A}_{d-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d-1}) \rightarrow \mathcal{A}_d/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_d) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a}).$$

It is a well-known result in commutative algebra that a finite tower of integral ring extensions is itself integral (see [AM69, Corollary 5.4]). Therefore, we get that

$$\mathcal{A}_{d-1}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d-1}) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$$

is integral. Injectivity of the above map is clear. This completes the proof. \square

We are now in a position to state and prove the main result: Theorem 17. We call Theorem 17 the discrete version of Noether's Normalization Lemma, or DNNL in short.

Theorem 17. (DNNL) *Let $\mathfrak{a} \subseteq \mathcal{A}$ be an ideal. Then there exists a coordinate transformation $T \in \mathbb{Z}^{n \times n}$ inducing the ring map $\varphi_T : \mathcal{A} \ni \sigma^\nu \mapsto \sigma^{T\nu} \in \mathcal{A}$ for all $\nu \in \mathbb{Z}^n$, and a positive integer $0 \leq d \leq n$ such that the canonical ring map*

$$\mathcal{A}_d \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$$

is injective and integral. Equivalently, the following two conditions hold:

- $\mathcal{A}/\varphi_T(\mathfrak{a})$ contains \mathcal{A}_d as a subring, and

- $\mathcal{A}/\varphi_T(\mathfrak{a})$ is a finitely generated module over \mathcal{A}_d .

Proof : As mentioned before, we give a proof by induction on the number $(n - d)$. The first step of the proof follows from Lemma 14. We may assume that $\mathfrak{a} \neq \{0\}$, because otherwise the theorem trivially holds with $d = n$. Since $\mathfrak{a} \neq \{0\}$, by Lemma 14 it follows that there exists $T_1 : \mathbb{Z}^{n \times n}$ unimodular such that

$$\mathcal{A}_{n-1}/(\varphi_{T_1}(\mathfrak{a}) \cap \mathcal{A}_{n-1}) \rightarrow \mathcal{A}/\varphi_{T_1}(\mathfrak{a})$$

is injective and integral. The inductive step is given by Lemma 16. If $\varphi_{T_1}(\mathfrak{a}) \cap \mathcal{A}_{n-1} = \{0\}$ then the result of the theorem follows with $d = n - 1$. On the other hand, if $\varphi_{T_1}(\mathfrak{a}) \cap \mathcal{A}_{n-1} \neq \{0\}$ then by Lemma 16 there exists unimodular $T_2 \in \mathbb{Z}^{n \times n}$ such that

$$\mathcal{A}_{n-2}/(\varphi_{T_2}(\varphi_{T_1}(\mathfrak{a})) \cap \mathcal{A}_{n-2}) \rightarrow \mathcal{A}/\varphi_{T_2}(\varphi_{T_1}(\mathfrak{a})) \quad (52)$$

is injective and integral. Note that $\varphi_{T_2} \circ \varphi_{T_1} = \varphi_{T_2 T_1}$. Thus equation (52) becomes

$$\mathcal{A}_{n-2}/(\varphi_{T_2 T_1}(\mathfrak{a}) \cap \mathcal{A}_{n-2}) \rightarrow \mathcal{A}/\varphi_{T_2 T_1}(\mathfrak{a})$$

is injective and integral. Next we look at $\varphi_{T_2 T_1}(\mathfrak{a}) \cap \mathcal{A}_{n-2}$. If this is the zero ideal then the theorem holds with $d = n - 2$. Otherwise, we once again invoke Lemma 16, by which we have $T_3 \in \mathbb{Z}^{n \times n}$ unimodular, such that

$$\mathcal{A}_{n-3}/(\varphi_{T_3 T_2 T_1}(\mathfrak{a}) \cap \mathcal{A}_{n-3}) \rightarrow \mathcal{A}/\varphi_{T_3 T_2 T_1}(\mathfrak{a})$$

is injective and integral. Then we look at $\varphi_{T_3 T_2 T_1}(\mathfrak{a}) \cap \mathcal{A}_{n-3}$ and depending on whether this ideal is the zero ideal or not we invoke Lemma 16 again or stop. We illustrate this process of recursively applying Lemma 16 in the following flow-chart Figure 1.

In the flow-chart, after the first step, if $\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-1} \neq \{0\}$ then Lemma 16 is applied recursively, and in the process i is incremented at each step. This recursive process continues as long as $\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-i} \neq \{0\}$. Note that the recursive process is guaranteed to stop after finitely many ($\leq n$) iterations because i is upper-bounded by n . When the process stops, we have the following situation

$$\mathcal{A}_{n-i}/(\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-i}) \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a}) \quad (53)$$

is injective and integral, plus $\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{n-i} = \{0\}$. This means we can rewrite equation (53) as

$$\mathcal{A}_{n-i} \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$$

is injective and integral. Defining $d := n - i$ we get our desired result. \square

Remark 18. The number d is of special importance to us. This number is equal to the *Krull dimension* of the Laurent polynomial ring \mathcal{A}_d . It is a known result in commutative algebra that the Krull dimensions of two commutative rings \mathcal{C}_1 and \mathcal{C}_2 are equal if $\mathcal{C}_1 \hookrightarrow \mathcal{C}_2$ is integral ([Eis95]). It then follows from Theorem 17 that the Krull dimension of $\mathcal{A}/\varphi_T(\mathfrak{a})$ too is equal to d . Yet another fact from commutative algebra says that Krull dimension remains invariant under isomorphism. Since φ_T is an automorphism of \mathcal{A} , \mathcal{A}/\mathfrak{a} and $\mathcal{A}/\varphi_T(\mathfrak{a})$ turn out to be isomorphic to each other as \mathbb{R} -algebras. Therefore, the Krull dimension of \mathcal{A}/\mathfrak{a} is d .

We illustrate the result of Theorem 17 in the following simple example.

Example 19. Consider the ideal $\mathfrak{a} = \langle \sigma_1 \sigma_2 - \sigma_1 - \sigma_2 + 1 \rangle \subseteq \mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]$. The quotient ring $\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]/\mathfrak{a}$ is not integral over either $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$ or $\mathbb{R}[\sigma_2, \sigma_2^{-1}]$. Theorem 17 tells us that with a coordinate change the quotient ring can be made integral over a smaller Laurent

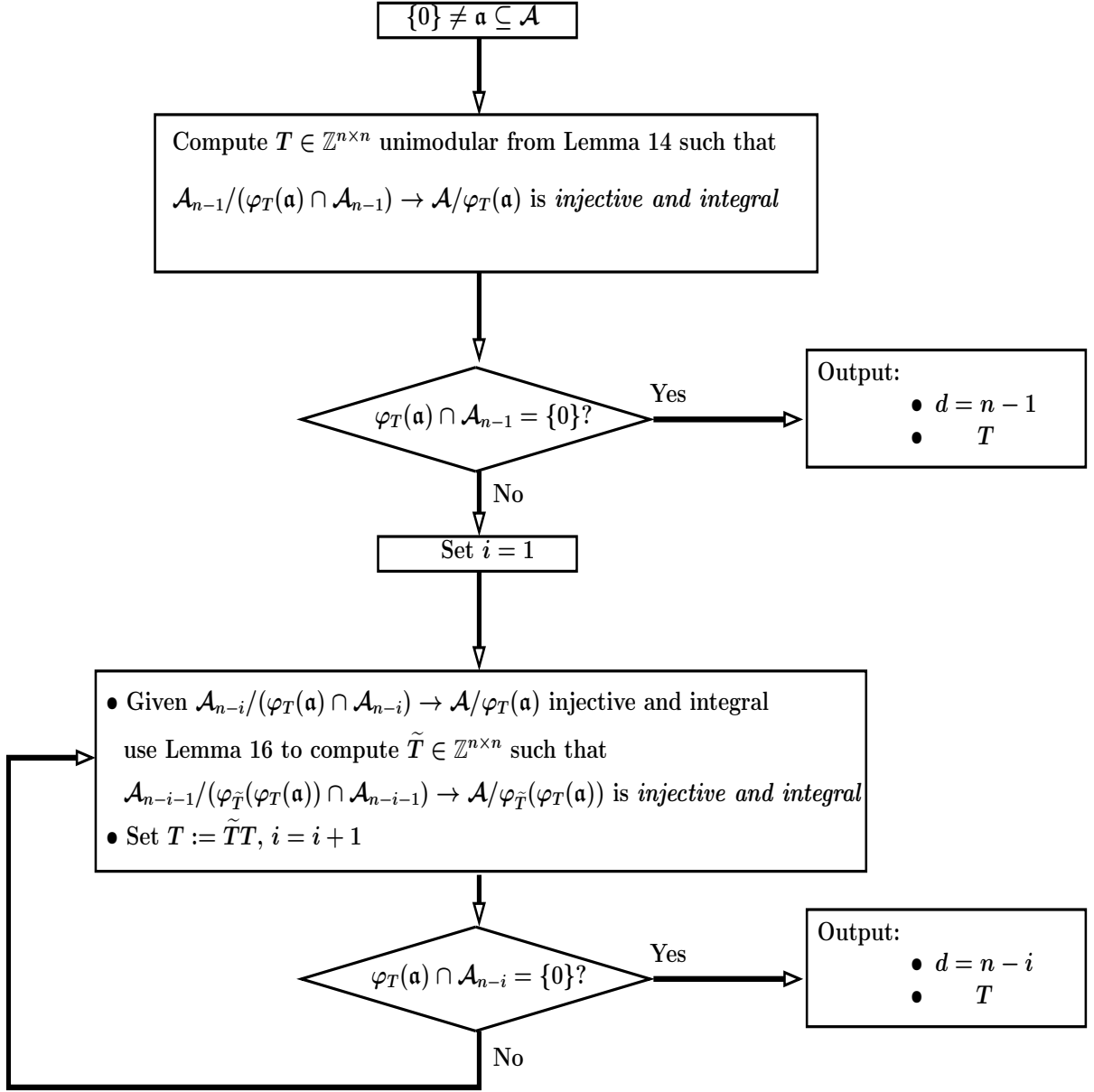


Figure 1: Flow-chart used in the proof of Theorem 17

polynomial ring. Note that $\dim(\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]/\mathfrak{a}) = 1$. So the first reduction in the flow-chart of Figure 1 yields the desired normalization. By Lemma 13 we can take $T \in \mathbb{Z}^{2 \times 2}$ to be

$$T = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

The corresponding φ_T turns out to be $\varphi_T : \sigma_1 \mapsto \sigma_1 \sigma_2^2, \sigma_2 \mapsto \sigma_2$. This φ_T maps the generator of \mathfrak{a} to

$$\varphi_T(\sigma_1 \sigma_2 - \sigma_1 - \sigma_2 + 1) = \sigma_1 \sigma_2^3 - \sigma_1 \sigma_2^2 - \sigma_2 + 1 = \sigma_1 (\sigma_2^3 - \sigma_2^2 - \sigma_1^{-1} \sigma_2 + \sigma_1^{-1}).$$

It then follows that $\varphi_T(\mathfrak{a}) = \langle \sigma_2^3 - \sigma_2^2 - \sigma_1^{-1} \sigma_2 + \sigma_1^{-1} \rangle$. Note that the generator of $\varphi_T(\mathfrak{a})$ is a monic polynomial in σ_2 with coefficients coming from $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$. In other words, $\overline{\sigma_2}$ in $\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]/\varphi_T(\mathfrak{a})$ satisfies a monic polynomial equation over $\mathbb{R}[\sigma_1, \sigma_1^{-1}]/(\varphi_T(\mathfrak{a}) \cap \mathbb{R}[\sigma_1, \sigma_1^{-1}])$. Moreover, $\varphi_T(\mathfrak{a}) \cap \mathbb{R}[\sigma_1, \sigma_1^{-1}]$ is clearly the zero ideal. Thus we get $\mathbb{R}[\sigma_1, \sigma_1^{-1}] \rightarrow \mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]/\varphi_T(\mathfrak{a})$ is injective and integral.

4.4 DNNL extended to modules

In this subsection we show how the normalization process can be extended to modules. This extension is essential in order to apply the normalization process to non-scalar systems. The extension of DNNL to modules is obtained by two crucial observations, which we elaborate now. In order to proceed further, we require the following algebraic object: the annihilator ideal of a quotient module \mathcal{M} , which is defined as follows:

$$\text{ann}(\mathcal{M}) = \{f(\boldsymbol{\sigma}) \in \mathcal{A} \mid f(\boldsymbol{\sigma})m = 0 \in \mathcal{M} \text{ for all } m \in \mathcal{M}\}. \quad (54)$$

Note that \mathcal{M} is *naturally*² a module over $\mathcal{A}/\text{ann}(\mathcal{M})$. Further, since the free module \mathcal{A}^q is of finite rank ($= q$) over \mathcal{A} , it is finitely generated as a module over \mathcal{A} . Now, \mathcal{M} , being a quotient of \mathcal{A}^q , is clearly finitely generated over \mathcal{A} . Hence, \mathcal{M} is finitely generated over $\mathcal{A}/\text{ann}(\mathcal{M})$ too. This is the first crucial observation.

The second observation involves the maps induced by a coordinate transformation of \mathbb{Z}^n . We write this observation as a proposition below.

Proposition 20. *Let $T \in \mathbb{Z}^{n \times n}$ be a \mathbb{Z} -unimodular matrix. Further, let φ_T and $\widehat{\varphi}_T$ be the two maps induced by T as in equations (38) and (39), respectively. Suppose $\mathcal{R} \subseteq \mathcal{A}^q$ is a submodule of the free module \mathcal{A}^q . Then the following holds:*

$$\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R})) = \text{ann}(\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})). \quad (55)$$

Proof : Note that $f(\boldsymbol{\sigma}) \in \text{ann}(\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R}))$ if and only if for all $r(\boldsymbol{\sigma}) \in \mathcal{A}^q$ we have $f(\boldsymbol{\sigma})r(\boldsymbol{\sigma}) \in \widehat{\varphi}_T(\mathcal{R})$. However, since $\widehat{\varphi}_T$ is a bijection, for every $r(\boldsymbol{\sigma}) \in \mathcal{A}^q$ there exists a unique $r_1(\boldsymbol{\sigma}) \in \mathcal{A}^q$ such that $\widehat{\varphi}_T(r_1(\boldsymbol{\sigma})) = r(\boldsymbol{\sigma})$. Therefore, we can write $f(\boldsymbol{\sigma}) \in \text{ann}(\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R}))$ if and only if for all $r_1(\boldsymbol{\sigma}) \in \mathcal{A}^q$ we have $f(\boldsymbol{\sigma})\widehat{\varphi}_T(r_1(\boldsymbol{\sigma})) \in \widehat{\varphi}_T(\mathcal{R})$. Recall that φ_T is an automorphism of \mathcal{A} . Therefore, there is a unique $g(\boldsymbol{\sigma}) := \varphi_T^{-1}(f(\boldsymbol{\sigma}))$. Then we can write

$$f(\boldsymbol{\sigma})\widehat{\varphi}_T(r_1(\boldsymbol{\sigma})) = \varphi_T(g(\boldsymbol{\sigma}))\widehat{\varphi}_T(r_1(\boldsymbol{\sigma})) = \widehat{\varphi}_T(g(\boldsymbol{\sigma})r_1(\boldsymbol{\sigma})) \in \widehat{\varphi}_T(\mathcal{R}) \Leftrightarrow g(\boldsymbol{\sigma}) \in \text{ann}(\cdot)$$

But $g(\boldsymbol{\sigma}) \in \text{ann}(\mathcal{A}^q/\mathcal{R})$ if and only if $f(\boldsymbol{\sigma}) \in \varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$. \square

We now present the non-scalar or module theoretic version of DNNL.

Theorem 21. (Module theoretic DNNL) *Let $\mathcal{R} \subseteq \mathcal{A}^q$ be a submodule. Suppose the Krull dimension of $\text{ann}(\mathcal{A}^q/\mathcal{R})$ is d . Then there exists a coordinate transformation $T \in \mathbb{Z}^{n \times n}$ inducing the \mathbb{R} -algebra homomorphism $\varphi_T : \mathcal{A} \ni \boldsymbol{\sigma}^\nu \mapsto \boldsymbol{\sigma}^{T\nu} \in \mathcal{A}$ for all $\nu \in \mathbb{Z}^n$, and the corresponding \mathcal{A} -module homomorphism $\widehat{\varphi}_T : \mathcal{A}^q \rightarrow \mathcal{A}^q$, such that the quotient module $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is a finitely generated module over \mathcal{A}_d .*

Proof : Let $T \in \mathbb{Z}^{n \times n}$ be an arbitrary \mathbb{Z} -unimodular integer matrix. We have already seen that for any submodule \mathcal{R} of \mathcal{A}^q , the quotient module $\mathcal{A}^q/\mathcal{R}$ is finitely generated as a module over $\mathcal{A}/\text{ann}(\mathcal{A}^q/\mathcal{R})$. In particular, since $\widehat{\varphi}_T(\mathcal{R})$ too is a submodule of \mathcal{A}^q we get that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is a finitely generated module over $\mathcal{A}/\text{ann}(\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R}))$. Now, let us define $\mathfrak{a} := \text{ann}(\mathcal{A}^q/\mathcal{R})$. By Proposition 20, $\varphi_T(\mathfrak{a}) = \text{ann}(\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R}))$. Therefore, $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is in fact a finitely generated module over $\mathcal{A}/\varphi_T(\mathfrak{a})$.

Since Krull dimension of \mathcal{A}/\mathfrak{a} is equal to d , by applying Theorem 17 to \mathfrak{a} we get that there exists a \mathbb{Z} -unimodular $T \in \mathbb{Z}^{n \times n}$ such that $\mathcal{A}/\varphi_T(\mathfrak{a})$ is a finitely generated module over \mathcal{A}_d . Thus, by combining this with the fact that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is a finitely generated module over $\mathcal{A}/\varphi_T(\mathfrak{a})$ we get the following chain of modules

$$\begin{array}{c} \mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R}) \\ \uparrow \\ \mathcal{A}/\varphi_T(\mathfrak{a}) \\ \uparrow \\ \mathcal{A}_d \end{array}$$

²‘Naturally’ here means the scalar multiplication for the base rings \mathcal{A} and $\mathcal{A}/\text{ann}(\mathcal{M})$ are identical.

where each step is finitely generated. Therefore, $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ must be finitely generated over \mathcal{A}_d . Indeed, suppose $\{g_1, \dots, g_k\} \subseteq \mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is a generating set for $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ as a module over $\mathcal{A}/\varphi_T(\mathfrak{a})$, and $\{h_1, \dots, h_\ell\} \subseteq \mathcal{A}/\varphi_T(\mathfrak{a})$ is a generating set for $\mathcal{A}/\varphi_T(\mathfrak{a})$ as a module over \mathcal{A}_d . Then

$$\{g_i h_j \mid 1 \leq i \leq k, 1 \leq j \leq \ell\}$$

is a generating set for $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ over \mathcal{A}_d . \square

We illustrate this result in the following example.

Example 22. Consider the submodule \mathcal{R} of $\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]^2$ generated by the rows of the matrix

$$R(\sigma) = \begin{bmatrix} \sigma_1 - 1 & 2 \\ 1 & \sigma_2 - 1 \end{bmatrix}.$$

It can be checked that the quotient module $\mathcal{M} = \mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]^2/\mathcal{R}$ is not finitely generated over $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$ or $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$, neither it is a finite dimensional vector space over \mathbb{R} . The annihilator ideal of the quotient module in this case turns out to be $\mathfrak{a} = \langle \sigma_1 \sigma_2 - \sigma_2 - \sigma_1 - 1 \rangle$. Take the unimodular matrix $T = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ for coordinate transformation. Then we get that under the ring map φ_T the ideal \mathfrak{a} is mapped to the ideal $\varphi_T(\mathfrak{a}) = \langle \sigma_1 \sigma_2^3 - \sigma_2 - \sigma_1 \sigma_2^2 - 1 \rangle$. Note that $\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]/\varphi_T(\mathfrak{a})$ is a finitely generated module over $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$.

The extension of φ_T to $\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]^2$, that is, $\widehat{\varphi}_T$ maps \mathcal{R} to the row-span of the following matrix:

$$\widetilde{R}(\sigma) = \begin{bmatrix} \sigma_1 \sigma_2^2 - 1 & 2 \\ 1 & \sigma_2 - 1 \end{bmatrix}.$$

Note that the annihilator of $\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]^2/\widehat{\varphi}_T(\mathcal{R})$ is given by $\varphi_T(\mathfrak{a})$. It then follows that $\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]^2/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated as a module over $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$. Indeed, it can be checked that,

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 0 \\ 1 \end{bmatrix}^T, \begin{bmatrix} \sigma_1 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 0 \\ \sigma_1 \end{bmatrix}^T, \begin{bmatrix} \sigma_1^2 \\ 0 \end{bmatrix}^T, \begin{bmatrix} 0 \\ \sigma_1^2 \end{bmatrix}^T \right\}$$

is a generating set for $\mathbb{R}[\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}]^2/\widehat{\varphi}_T(\mathcal{R})$ as a module over $\mathbb{R}[\sigma_1, \sigma_1^{-1}]$.

5 Representation formula for general autonomous systems

In this section we make use of Theorem 21 to obtain representation formula for general autonomous systems. This clearly is indicative of the fact that this representation formula that we are going to propose will involve a coordinate transformation on the indexing set \mathbb{Z}^n . Therefore, we first describe the effects of a coordinate transformation of \mathbb{Z}^n on the behavior of an n -D system.

Recall that a coordinate transformation of \mathbb{Z}^n is given by a \mathbb{Z} -unimodular matrix $T \in \mathbb{Z}^{n \times n}$ as

$$\begin{aligned} T : \mathbb{Z}^n &\rightarrow \mathbb{Z}^n \\ \text{col}(\nu_1, \nu_2, \dots, \nu_n) &=: \nu \mapsto T\nu. \end{aligned}$$

Now note that this T induces the following \mathbb{R} -linear map from $(\mathbb{R}^{\mathbb{Z}^n})^q$ to itself:

$$\begin{aligned} \Phi_T : (\mathbb{R}^{\mathbb{Z}^n})^q &\rightarrow (\mathbb{R}^{\mathbb{Z}^n})^q \\ w(\nu) &\mapsto w(T\nu), \end{aligned} \tag{56}$$

This map Φ_T is often called the *pull-back* of the coordinate transformation T . The pull-back Φ_T is a bijection because T is \mathbb{Z} -unimodular. In fact, it is easy to see that

$$\Phi_T^{-1} = \Phi_{T^{-1}}.$$

Recall the \mathbb{R} -algebra homomorphism $\varphi_T : \mathcal{A} \rightarrow \mathcal{A}$ induced by T , and its extension to modules $\widehat{\varphi}_T : \mathcal{A}^q \times \mathcal{A}^q$. The following lemma shows how $\widehat{\varphi}_T$ and the pull-back Φ_T are interrelated.

Lemma 23. *Let $v, w \in (\mathbb{R}^{\mathbb{Z}^n})^q$ be related by $v = \Phi_T(w)$. Then for $r(\sigma) \in \mathcal{A}^q$ we have*

$$r(\sigma)v = \Phi_T(\widehat{\varphi}_T(r(\sigma))w).$$

Proof : It is enough to prove for the scalar case: for $v, w \in \mathbb{R}^{\mathbb{Z}^n}$ and $f(\sigma) \in \mathcal{A}$ we must have

$$f(\sigma)v = \Phi_T(\varphi_T(f(\sigma))w). \quad (57)$$

This is because $\widehat{\varphi}_T$ is defined as φ_T applied element-wise, and Φ_T is linear. Further, note that every Laurent polynomial is a finite \mathbb{R} -linear combination of monomials. Therefore, once again by linearity of Φ_T , it is enough to prove equation (57) for $\mathcal{A} \ni f(\sigma) = \sigma^\nu$, where $\nu \in \mathbb{Z}^n$ is arbitrary.

Now, $v, w \in \mathbb{R}^{\mathbb{Z}^n}$ are assumed to be related by $v = \Phi_T(w)$. First note that for $\nu, \nu' \in \mathbb{Z}^n$, the action of the monomial σ^ν on v is given by the following

$$\begin{aligned} (\sigma^\nu v)(\nu') &= v(\nu' + \nu) = \Phi_T(w)(\nu' + \nu) = w(T(\nu' + \nu)) &= (\sigma^{T\nu}w)(T\nu') \\ &= \Phi_T(\varphi_T(\sigma^\nu)w)(\nu'). \end{aligned}$$

Since ν' was arbitrary we get for all $\nu \in \mathbb{Z}^n$

$$\sigma^\nu v = \Phi_T(\varphi_T(\sigma^\nu)w). \quad (58)$$

This is what we wanted to show. \square

With this we now bring out the effect of T on the behavior \mathfrak{B} of an n -D system. We show that the image of \mathfrak{B} under the pull-back Φ_T is also a behavior. Not only that, in fact, the equation modules of \mathfrak{B} and $\Phi_T(\mathfrak{B})$ are related by $\widehat{\varphi}_T$ in a way as shown in Proposition 24 below.

Proposition 24. *Let $\mathcal{R} \subseteq \mathcal{A}^q$ be a submodule with behavior $\mathfrak{B}(\mathcal{R})$, and let $T \in \mathbb{Z}^{n \times n}$ be \mathbb{Z} -unimodular. Then we have*

$$\Phi_T(\mathfrak{B}(\mathcal{R})) = \mathfrak{B}(\widehat{\varphi}_{T^{-1}}(\mathcal{R})). \quad (59)$$

Proof : Let $w \in (\mathbb{R}^{\mathbb{Z}^n})^q$ be an arbitrary n -D trajectory and let $r(\sigma) \in \mathcal{A}^q$ be an arbitrary row-vector of polynomial shift operators. Then, by Lemma 23, we have the following identity

$$r(\sigma)(\Phi_T(w)) = \Phi_T(\widehat{\varphi}_T(r(\sigma))w). \quad (60)$$

Since $\widehat{\varphi}_T$ and Φ_T both are bijective, it follows from equation (60) that $w \in \mathfrak{B}(\widehat{\varphi}_T(\mathcal{R}))$ if and only if $\Phi_T(w) \in \mathfrak{B}(\mathcal{R})$. In other words,

$$\Phi_{T^{-1}}(\mathfrak{B}(\mathcal{R})) = \mathfrak{B}(\widehat{\varphi}_T(\mathcal{R})).$$

Since T is invertible we can start the argument with T substituted by T^{-1} , and thus we obtain the desired equation (59). \square

Proposition 24 allows us to give the following definition.

Definition 25. (T -isomorphism of behaviors) *Suppose $\mathfrak{B}_1, \mathfrak{B}_2 \in \mathfrak{L}^q$. Then \mathfrak{B}_1 is said to be T -isomorphic to \mathfrak{B}_2 if there exists a \mathbb{Z} -unimodular matrix $T \in \mathbb{Z}^{n \times n}$ such that*

$$\mathfrak{B}_1 = \Phi_T(\mathfrak{B}_2).$$

Proposition 24 then translates in the language of Definition 25 to the following:

Corollary 26. *Let $\mathfrak{B}_1, \mathfrak{B}_2 \in \mathfrak{L}^q$ have their equation modules $\mathcal{R}_1, \mathcal{R}_2$, respectively. Then \mathfrak{B}_1 is T -isomorphic to \mathfrak{B}_2 if and only if $\mathcal{R}_1 = \hat{\varphi}_{T^{-1}}(\mathcal{R}_2)$, which in turn is true if and only if $\mathcal{R}_2 = \hat{\varphi}_T(\mathcal{R}_1)$.*

Combining Corollary 26 (or equivalently, Proposition 24) with the module theoretic DNNL (Theorem 21) we get the following important result.

Theorem 27. *Let $\mathfrak{B} \in \mathfrak{L}^q$ be an autonomous behavior with equation module $\mathcal{R} \subseteq \mathcal{A}^q$. Further, let the Krull dimension of $\text{ann}(\mathcal{A}^q/\mathcal{R})$ be equal to d . Then \mathfrak{B} is T -isomorphic to a strongly relevant autonomous system of order d .*

Proof : First note that, by Theorem 21, there exists a \mathbb{Z} -unimodular $T \in \mathbb{Z}^{n \times n}$ such that under the induced module map $\hat{\varphi}_T : \mathcal{A}^q \rightarrow \mathcal{A}^q$ we have $\mathcal{A}^q/\hat{\varphi}_T(\mathcal{R})$ a finitely generated module over \mathcal{A}_d . Therefore, $\mathfrak{B}(\hat{\varphi}_T(\mathcal{R}))$ is a strongly relevant autonomous behavior of order d , by Definition 2. By Corollary 26, \mathfrak{B} is T -isomorphic to $\mathfrak{B}(\hat{\varphi}_T(\mathcal{R}))$. Thus \mathfrak{B} is T -isomorphic to a strongly relevant autonomous system of order d . \square

Theorem 27 enables us to obtain the following representations for a general autonomous system. These representations follow from the representations of strongly relevant systems presented in Theorem 6 and Corollary 10. Recall the first order system of equations given in Table 1. The representations given below involve these equations. The next result is a consequence of Theorem 6.

Corollary 28. *Suppose $\mathfrak{B} \in \mathfrak{L}^q$ is an autonomous system with equation module \mathcal{R} . Let d be the Krull dimension of $\text{ann}(\mathcal{A}^q/\mathcal{R})$. Then, there exist a positive integer r and the following matrices:*

- $X(\sigma_1) \in \mathcal{A}_d^{\bullet \times r}$,
- $A_1(\sigma_1), A_2(\sigma_1), \dots, A_{n-d}(\sigma_1) \in \mathcal{A}_d^{r \times r}$,
- $C(\sigma_1) \in \mathcal{A}_d^{q \times r}$,

such that \mathfrak{B} admits the following representation:

$$\mathfrak{B} = \left\{ v \in (\mathbb{R}^{\mathbb{Z}^n})^q \mid \begin{array}{l} \exists \mathbf{x} \in (\mathbb{R}^{\mathbb{Z}^n})^r, w \in (\mathbb{R}^{\mathbb{Z}^n})^q \text{ such that equations in Table 1} \\ \text{are satisfied, and } v = \Phi_T(w) \end{array} \right\} \quad (61)$$

The next result is a consequence of Corollary 10

Corollary 29. *Let $\mathfrak{B} \in \mathfrak{L}^q$ be an autonomous system whose equation module is $\mathcal{R} \subseteq \mathcal{A}^q$. Suppose the Krull dimension of $\text{ann}(\mathcal{A}^q/\mathcal{R})$ is d . Then there exist*

- a positive integer r ,
- a matrix $X(\sigma_1) \in \mathcal{A}_d^{\bullet \times r}$,
- a set of $n - d$ square matrices $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1) \in \mathcal{A}_d^{r \times r}$,
- a matrix $C(\sigma_1) \in \mathcal{A}_d^{q \times r}$

such that \mathfrak{B} admits the following latent variable representation:

$$\mathfrak{B} = \left\{ v \in (\mathbb{R}^{\mathbb{Z}^n})^q \mid \begin{array}{l} \exists \mathbf{x} \in (\mathbb{R}^{\mathbb{Z}^n})^r \text{ and } w \in (\mathbb{R}^{\mathbb{Z}^n})^q \text{ satisfying} \\ \begin{bmatrix} X(\sigma_1) & \vdots & 0 \\ \sigma_{d+1}I_r - A_1(\sigma_1) & \vdots & 0 \\ \sigma_{d+2}I_r - A_2(\sigma_1) & \vdots & 0 \\ \vdots & \vdots & \vdots \\ \sigma_n I_r - A_{n-d}(\sigma_1) & \vdots & 0 \\ -C(\sigma_1) & \vdots & I_q \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ w \end{bmatrix} = 0, \quad v = \Phi_T(w) \end{array} \right\} \quad (62)$$

With these representations for general autonomous systems, we are now in a position to provide an algorithm for finding solutions for general autonomous systems. The algorithm is exactly the same as Algorithm 11 with one extra stage at the beginning, where we *normalize* the given system to a T -isomorphic system that is strongly relevant.

Algorithm 30. (Solution formula for general autonomous systems)

(Noether) Normalization	
Input: An autonomous system $\mathfrak{B} = \ker(R(\sigma))$, where $R(\sigma) \in \mathcal{A}^{\bullet \times q}$.	
Computation: Define $\mathcal{R} = \text{rowspan}(R(\sigma)) \subseteq \mathcal{A}^q$. Obtain $\mathfrak{a} = \text{ann}(\mathcal{A}^q/\mathcal{R})$. Using Theorem 17 find out a \mathbb{Z} -unimodular $T \in \mathbb{Z}^{n \times n}$ such that under the induced map $\varphi_T : \mathcal{A} \rightarrow \mathcal{A}$ we have $\mathcal{A}_d \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$ injective and integral.	
Output: T . $\tilde{\mathcal{R}} := \hat{\varphi}_T(\mathcal{R})$.	
Regularization	
Input: $\tilde{\mathcal{R}} \subseteq \mathcal{A}^q$.	
Computation: Obtain a generating set $\mathcal{G} := \{g_1, \dots, g_r\} \subseteq \mathcal{A}^q/\tilde{\mathcal{R}}$. Obtain the matrix of relations $X(\sigma_1) \in \mathcal{A}_d^{k \times r}$. Obtain the companion matrices $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1) \in \mathcal{A}_d^{r \times r}$ (ensure that these matrices are invertible in \mathcal{A}_d). Obtain the output matrix $C(\sigma_1) \in \mathcal{A}_d^{q \times r}$.	
Output: The matrices $X(\sigma_1)$, $A_1(\sigma_1), \dots, A_{n-d}(\sigma_1)$, and $C(\sigma_1)$.	
Recursion	
Input: <i>The set of initial data:</i> Solve $X(\sigma_1)x = 0$ for $x \in \left(\mathbb{R}^{\mathbb{Z}^d}\right)^r$.	
Computation: for $\nu = (\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$ set $\tilde{w}(\nu) = \left(C(\sigma_1) \prod_{i=1}^{n-d} A_i(\sigma_1)^{\nu_{d+i}} x \right) (\nu_1, \nu_2, \dots, \nu_d).$ end	
Output: The sequence $\tilde{w} := \{\tilde{w}(\nu)\}_{\nu \in \mathbb{Z}^n}$.	
Renormalization	
Input: The sequence $\tilde{w} := \{\tilde{w}(\nu)\}_{\nu \in \mathbb{Z}^n}$.	
Computation: for $\nu = (\nu_1, \nu_2, \dots, \nu_n) \in \mathbb{Z}^n$ set $w(\nu) = \tilde{w}(T\nu).$ end	
Output: The sequence $w := \{w(\nu)\}_{\nu \in \mathbb{Z}^n}$.	

6 The set of allowable initial conditions

In Algorithms 11 and 30, the initial conditions $x \in \left(\mathbb{R}^{\mathbb{Z}^d}\right)^r$ are required to satisfy the equation $X(\sigma_1)x = 0$. This is in contrast with the 1-D situation, where one can *always* choose x in such a way that the set of initial conditions is free (see [Wil83]). In this section we analyze the set of allowable initial conditions and address certain important issues, namely, *freeness* of the initial conditions, and *non-autonomy* of the state space \mathcal{X} .

6.1 Freeness of the set of allowable initial conditions

We have already seen that the representation of an autonomous system given by Theorem 6 can be viewed as an $(n - d)$ -D flow equation arising out of an $(n - d)$ -D first order dynamics on an infinite dimensional space. We start by identifying this infinite dimensional space. Suppose $\mathcal{R} \subseteq \mathcal{A}^q$ is a submodule such that $\mathcal{A}^q/\mathcal{R}$ is a finitely generated module over \mathcal{A}_d . We fix a generating set $\{g_1, \dots, g_r\}$ for $\mathcal{A}^q/\mathcal{R}$ as an \mathcal{A}_d -module. Recall equation (9), where we identified $\mathcal{A}^q/\mathcal{R}$ with a quotient module of \mathcal{A}_d^r via the map $\psi : \mathcal{A}_d^r \rightarrow \mathcal{A}^q/\mathcal{R}$. Let $X(\sigma_1) \in \mathcal{A}_d^{k \times r}$ be a matrix of relations of $\{g_1, \dots, g_r\}$. We have defined the following set of vector valued d -D trajectories:

$$\mathcal{X} := \left\{ x \in \left(\mathbb{R}^{\mathbb{Z}^d} \right)^r \mid X(\sigma_1)x = 0 \right\}, \quad (63)$$

as the state space.

It is clear that \mathcal{X} contains all the allowable initial conditions. Note that \mathcal{X} is in fact a vector valued d -D behavior having $X(\sigma_1)$ as a kernel representation matrix. The submodule corresponding to this behavior is the row-span of the matrix $X(\sigma_1)$ over \mathcal{A}_d , which equals $\ker(\psi)$. Clearly, this submodule $\ker(\psi)$ is unique for given set of generators of $\mathcal{A}^q/\mathcal{R}$ as a module over \mathcal{A}_d . Thus, by the one-to-one correspondence between behaviors and submodules, \mathcal{X} gets fixed once a generating set for $\mathcal{A}^q/\mathcal{R}$ (as an \mathcal{A}_d -module) is fixed. However, even for a fixed \mathcal{R} , different generating sets for $\mathcal{A}^q/\mathcal{R}$ as a \mathcal{A}_d -module may exist. These different generating sets may even have different modules of relations, leading to distinct \mathcal{X} s. But, it can be shown that these different \mathcal{X} s are *isomorphic* to each other in the sense of [PWR02], because they have isomorphic quotient modules. One important question related to \mathcal{X} is: when does $\mathcal{A}^q/\mathcal{R}$ admit a generating set of cardinality r such that the corresponding \mathcal{X} equals the whole of $\left(\mathbb{R}^{\mathbb{Z}^d} \right)^r$? In the sequel, we refer to this situation by saying $\mathcal{A}^q/\mathcal{R}$ *admits a free \mathcal{X} of rank r* .

It is easy to see that the answer to this question is: if and only if $\mathcal{A}^q/\mathcal{R}$ is a *free module of rank r over \mathcal{A}_d* . This is because then, and only then, $\mathcal{A}^q/\mathcal{R}$ will admit a free generating set, i.e., the matrix of relations $X(\sigma_1)$ corresponding to the generating set will be the zero matrix. And consequently, \mathcal{X} will be the whole of $\left(\mathbb{R}^{\mathbb{Z}^d} \right)^r$. This fact together with Swan's extension [Swa78] of Serre conjecture to Laurent polynomial rings give us the following check (Theorem 32) for determining whether $\mathcal{A}^q/\mathcal{R}$ admits a free \mathcal{X} or not.

Remark 31. In Theorem 32 we require the notion of a *zero left-prime* Laurent polynomial matrix. A Laurent polynomial matrix $X(\sigma_1) \in \mathcal{A}_d^{k \times r}$ having full row rank is said to be *zero left-prime* if the ideal generated by the $(k \times k)$ minors of $X(\sigma_1)$ is the whole ring \mathcal{A}_d . See [Zer99, Bos82] for various different notions of prime-ness and their significances. One particular property of zero left-prime matrices that will be important for proving Theorem 32 is the following:

The row-span of a zero left-prime matrix is a direct-summand of the corresponding free module. And, conversely, if a submodule \mathcal{R} of the free module \mathcal{A}^q is a direct-summand then \mathcal{R} admits representation as the row-span of a matrix that is zero left-prime [Zer99, Bos82].

Theorem 32. *Let $\mathcal{R} \subseteq \mathcal{A}^q$ be a submodule such that $\mathcal{A}^q/\mathcal{R}$ is a finitely generated module over \mathcal{A}_d . Fix any generating set $\{g_1, \dots, g_r\}$ for $\mathcal{A}^q/\mathcal{R}$ as an \mathcal{A}_d -module. Then $\mathcal{A}^q/\mathcal{R}$ admits a free \mathcal{X} of rank r' for some $r' \in \mathbb{N}$ if and only if the generators $\{g_1, \dots, g_r\}$ admit a matrix of relations $X(\sigma_1) \in \mathcal{A}_d^{k \times r}$ which is zero left-prime.*

Proof : Recall the map $\psi : \mathcal{A}_d^r \rightarrow \mathcal{A}^q/\mathcal{R}$ from equation (9) and note that $\mathcal{A}^q/\mathcal{R}$ is isomorphic to $\mathcal{A}_d^r/\ker(\psi)$ as \mathcal{A}_d -modules. Now, as seen above, $\mathcal{A}^q/\mathcal{R}$ admits a free \mathcal{X} of rank r' if and only if $\mathcal{A}^q/\mathcal{R}$ is a free \mathcal{A}_d -module (of rank r'). By Swan's extension of Serre's conjecture to Laurent polynomial rings, $\mathcal{A}^q/\mathcal{R}$ is a free \mathcal{A}_d -module if and only if $\mathcal{A}^q/\mathcal{R}$ is a *projective* \mathcal{A}_d -module.

Since $\mathcal{A}^q/\mathcal{R}$ is isomorphic to $\mathcal{A}_d^r/\ker(\psi)$ as \mathcal{A}_d -modules, $\mathcal{A}^q/\mathcal{R}$ being projective is equivalent to $\mathcal{A}_d^r/\ker(\psi)$ being projective. This, in turn, is equivalent to splitting of the following short exact sequence of \mathcal{A}_d -modules ([Eis95]):

$$0 \rightarrow \ker(\psi) \rightarrow \mathcal{A}_d^r \rightarrow \mathcal{A}_d^r/\ker(\psi) \rightarrow 0.$$

This is true if and only if $\ker(\psi)$ is a direct summand of \mathcal{A}_d^r ([Eis95]). But, a submodule of the free module \mathcal{A}_d^r is a direct summand if and only if it admits representation as the row-span of a zero left-prime matrix (see Remark 31). Thus, $\ker(\psi)$ being a direct summand of \mathcal{A}_d^r is equivalent to existence of an $X(\boldsymbol{\sigma}_1) \in \mathcal{A}_d^{k \times r}$ such that

$$\ker(\psi) = \text{rowspan}(X(\boldsymbol{\sigma}_1)),$$

where $X(\boldsymbol{\sigma}_1)$ is zero left-prime. □

Remark 33. The significance of having a free \mathcal{X} is that initial conditions can then be chosen arbitrarily. That is, solutions in $\mathfrak{B}(\mathcal{R})$ can then all be obtained by Algorithm 11 with arbitrary $x \in (\mathbb{R}^{\mathbb{Z}^d})^r$. Note that in Theorem 32 it has been assumed that the behavior is strongly relevant. Therefore, in order to check freeness of initial conditions for a general system, one must first apply a suitable Noether's normalization, and then invoke Theorem 32. This brings up the question whether freeness of initial condition is dependent on the particular normalization used, or is it an inherent property of the original system. This remains an interesting open question.

6.2 Non-autonomy of the set of allowable initial conditions

As mentioned above, the set of allowable initial conditions, or the state-space, \mathcal{X} can be viewed as a d -D behavior itself. It is often desirable to have this d to be as small as possible. We show in this subsection that this question of whether d is the smallest possible or not is related with \mathcal{X} being non-autonomous as a d -D behavior.

It is already well-known that an n -D behavior \mathfrak{B} is non-autonomous if and only if the quotient module $\mathcal{A}^q/\mathcal{R}$ is *faithful*³ over \mathcal{A} . Translated to the case of \mathcal{X} it means \mathcal{X} is non-autonomous if and only if $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is faithful as an \mathcal{A}_d -module. Keeping this observation in mind, it is then desirable to design the coordinate transformation T so as to ensure $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is faithful as an \mathcal{A}_d -module. It so happens that our proof of the module theoretic DNNL (Theorem 21) already guarantees this property for $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$. We bring out this fact in the following Proposition 34, which is a slightly modified version of Theorem 21.

Proposition 34. *Let $\mathcal{R} \subseteq \mathcal{A}^q$ be a submodule. Suppose the Krull dimension of $\text{ann}(\mathcal{A}^q/\mathcal{R})$ is d . Then there exists a coordinate transformation $T \in \mathbb{Z}^{n \times n}$ inducing the \mathbb{R} -algebra homomorphism $\varphi_T : \mathcal{A} \ni \boldsymbol{\sigma}^\nu \mapsto \boldsymbol{\sigma}^{T\nu} \in \mathcal{A}$ for all $\nu \in \mathbb{Z}^n$, and the corresponding \mathcal{A} -module homomorphism $\widehat{\varphi}_T : \mathcal{A}^q \rightarrow \mathcal{A}^q$, such that the quotient module $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is a finitely generated and faithful module over \mathcal{A}_d .*

Proof : Recall the proof of Theorem 21. We have already seen there that a unimodular $T \in \mathbb{Z}^{n \times n}$ that makes $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ a finitely generated module over \mathcal{A}_d can be constructed using Theorem 17: a unimodular $T \in \mathbb{Z}^{n \times n}$ which renders $\mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$ finitely generated module over \mathcal{A}_d suffices. However, the T constructed in Theorem 17 does more; it makes the canonical map $\mathcal{A}_d \rightarrow \mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$ injective and integral. This means the T constructed in Theorem 17 not only makes $\mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$ finitely generated over \mathcal{A}_d , but faithful over \mathcal{A}_d , too. In other words, by Theorem 17, there exists $T \in \mathbb{Z}^{n \times n}$ unimodular

³A module \mathcal{M} over \mathcal{A} is said to be *faithful* if $\text{ann}(\mathcal{M}) = \{0\}$.

such that $\mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}/\mathcal{R}))$ is finitely generated and faithful as a module over \mathcal{A}_d . However, $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is clearly a faithful module over $\mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$. Thus $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is faithful over \mathcal{A}_d . That $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated over \mathcal{A}_d has already been proved in Theorem 21. \square

Combining this observation with the fact that \mathcal{X} is non-autonomous if and only if $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is faithful over \mathcal{A}_d , we get the following interesting result.

Corollary 35. *Let $\mathfrak{B} \in \mathfrak{L}^q$ be an autonomous n -D system such that the Krull dimension of $\mathcal{A}/\text{ann}(\mathcal{A}^q/\mathcal{R})$ is equal to d . Then there exists a unimodular $T \in \mathbb{Z}^{n \times n}$ such that*

1. \mathfrak{B} is T -isomorphic to a strongly relevant autonomous system \mathfrak{B}_2 of order d , and
2. the state space \mathcal{X} corresponding to \mathfrak{B}_2 is non-autonomous as a d -D behavior.

We have claimed in the beginning of this subsection that non-autonomy of \mathcal{X} is related with the smallest possible d . In order to prove this claim we first show that if the Krull dimension of $\mathcal{A}/\text{ann}(\mathcal{A}^q/\mathcal{R})$ is equal to d then $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ cannot be finitely generated as a module over $\mathcal{A}_{d'}$ for any $d' < d$. In other words, for the existence of a d' -D behavior \mathcal{X} it is necessary that $d' \geq d$.

Proposition 36. *Let $\mathcal{R} \subseteq \mathcal{A}^q$ be a submodule. Suppose the Krull dimension of $\mathcal{A}/\text{ann}(\mathcal{A}^q/\mathcal{R})$ is equal to d . Then there exists a unimodular $T \in \mathbb{Z}^{n \times n}$ such that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated as a module over $\mathcal{A}_{d'}$ if and only if $d' \geq d$.*

Proof : **(If)** We assume that $d' \geq d$, and we want to show that there exists a unimodular $T \in \mathbb{Z}^{n \times n}$ such that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated as a module over $\mathcal{A}_{d'}$. This is an immediate consequence of Theorem 21 (or Proposition 34). Indeed, by Theorem 21 there exists a unimodular $T \in \mathbb{Z}^{n \times n}$ such that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated as a module over \mathcal{A}_d . However, since $d' \geq d$ means \mathcal{A}_d is a subring of $\mathcal{A}_{d'}$, $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ clearly is finitely generated as a module over $\mathcal{A}_{d'}$, too.

(Only if) We assume that there exists a unimodular $T \in \mathbb{Z}^{n \times n}$ such that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated as a module over $\mathcal{A}_{d'}$, and we want to show that $d' \geq d$. Let us define $\mathfrak{a} := \text{ann}(\mathcal{A}^q/\mathcal{R})$. Recall from Proposition 20 that $\varphi_T(\mathfrak{a}) = \text{ann}(\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R}))$. Since $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated as a module over $\mathcal{A}_{d'}$, we get that $\mathcal{A}/\text{ann}(\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R}))\mathfrak{a}$ is also finitely generated as an $\mathcal{A}_{d'}$ -module. Therefore, by the identity of Proposition 20, $\mathcal{A}/\varphi_T(\mathfrak{a})$ is finitely generated as a module over $\mathcal{A}_{d'}$. Therefore, the canonical map $\mathcal{A}_{d'}/\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d'} \rightarrow \mathcal{A}/\varphi_T(\mathfrak{a})$ is injective integral (see Remark 15). Thus Krull dimension of $\mathcal{A}/\varphi_T(\mathfrak{a})$ is equal to that of $\mathcal{A}_{d'}/\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d'}$, but Krull dimension of $\mathcal{A}_{d'}/\varphi_T(\mathfrak{a}) \cap \mathcal{A}_{d'}$ is clearly less than or equal to that of $\mathcal{A}_{d'}$, which is d' . Again, Krull dimension of $\mathcal{A}/\varphi_T(\mathfrak{a})$ is d because $\mathcal{A}/\varphi_T(\mathfrak{a})$ and \mathcal{A}/\mathfrak{a} are isomorphic (see Remark 15). Therefore, $d' \geq d$. \square

Next we show that if $d' > d$ the Krull dimension of $\mathcal{A}/\text{ann}(\mathcal{A}^q/\mathcal{R})$, then the corresponding \mathcal{X} cannot be non-autonomous.

Lemma 37. *Let $\mathcal{R} \subseteq \mathcal{A}^q$ be a submodule. Suppose the Krull dimension of $\mathcal{A}/\text{ann}(\mathcal{A}^q/\mathcal{R})$ is equal to d . Further, let $T \in \mathbb{Z}^{n \times n}$ be unimodular such that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated as a module over $\mathcal{A}_{d'}$. If $d' > d$ then $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ cannot be faithful as a module over $\mathcal{A}_{d'}$.*

Proof : Suppose, contrary to the claim, that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is faithful as a module over $\mathcal{A}_{d'}$. Then the annihilator of $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ as a module over $\mathcal{A}_{d'}$, which is $\text{ann}(\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})) \cap \mathcal{A}_{d'}$, must be $\{0\}$. Utilizing the identity of Proposition 20 we get

$$\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R})) \cap \mathcal{A}_{d'} = \{0\}.$$

However, this means that the canonical map $\mathcal{A}_{d'} \rightarrow \mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$ is injective. Further, as has been argued in the proof of Proposition 36, $\mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$ is finitely generated over $\mathcal{A}_{d'}$ because $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is so. Therefore, the canonical map $\mathcal{A}_{d'} \rightarrow \mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$ is integral, too. Therefore, Krull dimension of $\mathcal{A}/\varphi_T(\text{ann}(\mathcal{A}^q/\mathcal{R}))$ must be equal to that of $\mathcal{A}_{d'}$, which happens to be d' . This clearly contradicts the assumption that $d' > d$. \square

These observations can be summed up as follows:

Theorem 38. *Let $\mathfrak{B} \in \mathfrak{L}^q$ be an autonomous behavior with equation module $\mathcal{R} \subseteq \mathcal{A}^q$. Let d be the Krull dimension of $\mathcal{A}/\text{ann}(\mathcal{A}^q/\mathcal{R})$. Then there exists a unimodular $T \in \mathbb{Z}^{n \times n}$ such that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated over $\mathcal{A}_{d'}$ with the corresponding state space \mathcal{X} non-autonomous if and only if d' is equal to d .*

Proof : **(If)** This implication is just a restatement of Corollary 35.

(Only if) By Proposition 36, $d' \not\leq d$; for in that case no unimodular $T \in \mathbb{Z}^{n \times n}$ exists such that $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ is finitely generated over $\mathcal{A}_{d'}$. On the other hand, if $d' > d$ then, by Lemma 37, $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ cannot be faithful over $\mathcal{A}_{d'}$, which means \mathcal{X} cannot be non-autonomous. Therefore, $d' = d$. \square

7 Concluding remarks

In this paper, we presented novel representation formulae for solutions of discrete n -D autonomous systems. Our analysis is based on a crucial algebraic property: the quotient module being finitely generated over a proper subring of the ring of shift operators, \mathcal{A} . Quite expectedly, many systems do not have this property. Therefore, we first consider those systems whose quotient modules are indeed finitely generated over a subring \mathcal{A}_d . We called such systems *strongly relevant of order d* . We then showed that such systems admit a state space like first order evolutionary equations. Using this we provided an explicit solution formula for trajectories in such systems. Next, we considered systems that are not strongly relevant. For these systems we showed that they can be converted to strongly relevant ones by a suitable change of coordinates on the indexing set \mathbb{Z}^n . The crucial fact that enables this conversion is what we have called the discrete version of Noether's normalization lemma (DNNL). We showed in this paper that given any submodule $\mathcal{R} \subseteq \mathcal{A}^q$, there exists a coordinated transformation $T : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ such that, under the corresponding module homomorphism $\widehat{\varphi}_T(\mathcal{R})$, the quotient module $\mathcal{A}^q/\widehat{\varphi}_T(\mathcal{R})$ becomes finitely generated as a module over a subring \mathcal{A}_d . Using this DNNL we have shown how a general discrete n -D autonomous system can be converted to a strongly relevant system. Then, making use of the earlier representation formula for solutions of strongly relevant systems, and the inverse of the coordinate transformation we obtained representation formula for general discrete n -D autonomous systems.

An interesting feature of the representation formulae presented in this paper is that the solution trajectories are obtained by making $(n-d)$ -D flow operators acting on initial conditions that are trajectories defined over \mathbb{Z}^d . This is very much akin to the state space solution formula of 1-D systems. However, there is one crucial deviation: unlike 1-D systems, here it may not always be possible to choose the initial conditions freely. In this paper, we provide necessary and sufficient conditions for these initial conditions to be free. Another interesting question concerning the set of allowable initial conditions is that whether it can be made smaller. This issue is related with the number d . We show in this paper that the smallest value that the number d can take is equal to the dimension of the characteristic variety of the system.

Many important questions relevant to the results presented in this paper have been left unanswered. For example: can the representation formulae be extended to non-autonomous systems? Another relevant question is: what is the minimum number of state variables? Is

this number intrinsic to the system, or does it depend on the coordinate transformation? We have also not answered questions concerning how existing computer algebra packages can be used to compute the various matrices used in the representation formulae.

Appendix

Proof of Lemma 4

In order to prove Lemma 4 we need the following algebraic result: Lemma 39. Lemma 39 follows from elementary commutative algebra. However, for a direct proof of Lemma 39, the reader may refer to [PP13], where $n = 2, d = 1$ case of the result has been proved. The extension to the general n, d case is straightforward, and hence we skip it here.

Lemma 39. *The following are equivalent.*

1. $\mathcal{A}^q/\mathcal{R}$ is finitely generated over \mathcal{A}_d .
2. For every $1 \leq i \leq n - d$ there exists a polynomial $p_i(\sigma) \in \text{ann}(\mathcal{A}^q/\mathcal{R})$ of the form

$$\sigma_{d+i}^{L_i} + a_{i,L_i-1}(\sigma_1)\sigma_{d+i}^{L_i-1} + \cdots + a_{i,1}(\sigma_1)\sigma_{d+i} + a_{i,0}(\sigma_1), \quad (64)$$

where L_i is a finite positive integer, $a_{i,j}(\sigma_1) \in \mathcal{A}_d$ for all $1 \leq i \leq n - d$ and $1 \leq j \leq L_i - 1$, with $a_{i,0}(\sigma_1)$ a unit for all $1 \leq i \leq n - d$.

3. For every $1 \leq i \leq n - d$ there exists a polynomial $p_i(\sigma) \in \mathcal{A}$ of the form

$$\sigma_{d+i}^{L_i} + a_{i,L_i-1}(\sigma_1)\sigma_{d+i}^{L_i-1} + \cdots + a_{i,1}(\sigma_1)\sigma_{d+i} + a_{i,0}(\sigma_1), \quad (65)$$

where L_i is a finite positive integer, $a_{i,j}(\sigma_1) \in \mathcal{A}_d$ for all $1 \leq i \leq n - d$ and $1 \leq j \leq L_i - 1$, with $a_{i,0}(\sigma_1)$ a unit for all $1 \leq i \leq n - d$, such that

$$p_i(\sigma)e_j \in \mathcal{R}$$

for all $1 \leq j \leq q$.

With the help of Lemma 39 we now prove Lemma 4

Proof of Lemma 4: **Part (1)** This assertion follows from repeated application of Lemma 3, and the fact that the maps μ_j commute pairwise.

Part (2) We first prove the result for the special case when $q = 1$.

Case 1 ($q = 1$): In this case $\mathcal{R} \subseteq \mathcal{A}$ is an ideal, and hence, $\text{ann}(\mathcal{A}/\mathcal{R}) = \mathcal{R}$. Recall that Lemma 4 deals with the situation when \mathcal{A}/\mathcal{R} is finitely generated as a module over \mathcal{A}_d . Therefore, by Lemma 39, for every $1 \leq i \leq n - d$ there exists a polynomial $p_i(\sigma) \in \mathcal{R}$ having the following form

$$\sigma_{d+i}^{L_i} + a_{i,L_i-1}(\sigma_1)\sigma_{d+i}^{L_i-1} + \cdots + a_{i,1}(\sigma_1)\sigma_{d+i} + a_{i,0}(\sigma_1),$$

where L_i is a finite positive integer, $a_{i,j}(\sigma_1) \in \mathcal{A}_d$ for all $1 \leq i \leq n - d$ and $1 \leq j \leq L_i - 1$, with $a_{i,0}(\sigma_1)$ a unit in \mathcal{A}_d for all $1 \leq i \leq n - d$.

Now consider a Laurent monomial σ_{d+i}^ν where $\nu \in \mathbb{Z}$. Since $p_i(\sigma)$ is monic in σ_{d+i} and its coefficient for the zeroth power of σ_{d+i} is a unit in \mathcal{A}_d , we can carry out long division of σ_{d+i}^ν by $p_i(\sigma)$ to get

$$\sigma_{d+i}^\nu = q(\sigma)p_i(\sigma) + b_{i,L_i-1}(\sigma_1)\sigma_{d+i}^{L_i-1} + b_{i,L_i-2}(\sigma_1)\sigma_{d+i}^{L_i-2} + \cdots + b_{i,1}(\sigma_1)\sigma_{d+i} + b_{i,0}(\sigma_1).$$

In other words, σ_{d+i}^ν is congruent modulo \mathcal{R} to an \mathcal{A}_d -linear combination of $\{1, \sigma_{d+i}, \sigma_{d+i}^2, \dots, \sigma_{d+i}^{L_i-1}\}$.

Notice that the above mentioned procedure can be carried out for all $1 \leq i \leq n-d$. Hence it follows that a Laurent monomial of the form $\prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_i}$ is congruent modulo \mathcal{R} to an \mathcal{A}_d -linear combination of the following monomials:

$$\mathcal{G} := \left\{ \prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_i} \mid 0 \leq \nu_i \leq L_i - 1 \right\}. \quad (66)$$

(The indices of the monomials in \mathcal{G} correspond to the parallelepiped, in the positive orthant of the integer grid \mathbb{Z}^{n-d} , with sides having lengths $L_1 - 1, L_2 - 1, \dots, L_{n-d} - 1$ units. See Figure 2.) Since every Laurent polynomial is an \mathcal{A}_d -linear combination of monomials of the form $\prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_i}$, it follows now that every Laurent polynomial is congruent modulo \mathcal{R} to an \mathcal{A}_d -linear combination of monomials in \mathcal{G} .

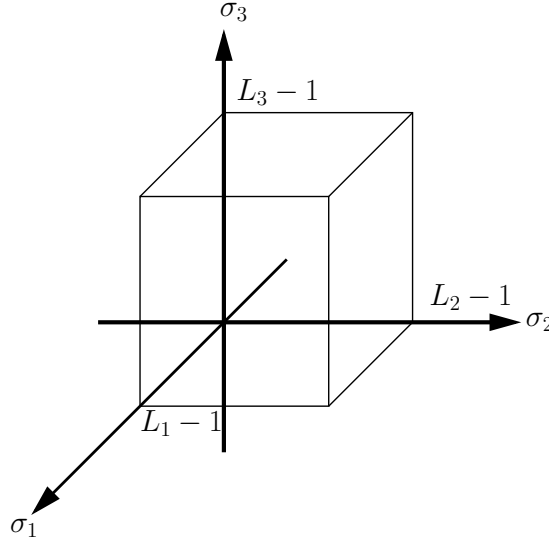


Figure 2: The parallelepiped when $n - d = 3$

Hence, the images of the elements in \mathcal{G} under the canonical map $\mathcal{A} \rightarrow \mathcal{A}/\mathcal{R}$ forms a generating set of \mathcal{A}/\mathcal{R} as a module over \mathcal{A}_d . We denote this set of images by $\overline{\mathcal{G}}$. We claim that under this generating set μ_i 's admit matrix representations that are all unimodular over \mathcal{A}_d .

We first show that μ_1 has a matrix representation $A_1(\sigma_1)$ that is unimodular. In order to do this we first put an ordering of the elements in \mathcal{G} . Consider the lexicographic ordering of monomials with $\sigma_{d+1} \prec \sigma_{d+2} \prec \dots \prec \sigma_n$, and write down the elements of \mathcal{G} in descending order. Let us name the elements of $\overline{\mathcal{G}}$, in this order, as $\{g_1, g_2, \dots, g_L\}$, where $L = \prod_{i=1}^{n-d} L_i$. Now, note that when the generators are ordered like this then they satisfy the following set of equations:

$$\begin{aligned} \mu_1(g_1) &= g_2 \\ &\vdots \\ \mu_1(g_{L_1}) &= -a_{1,0}(\sigma_1)g_1 - a_{1,1}(\sigma_1)g_2 - \dots - a_{1,L_1-1}(\sigma_1)g_{L_1} \\ \mu_1(g_{L_1+1}) &= g_{L_1+2} \\ &\vdots \\ \mu_1(g_{2L_1}) &= -a_{1,0}(\sigma_1)g_{L_1} - a_{1,1}(\sigma_1)g_{L_1+1} - \dots - a_{1,L_1-1}(\sigma_1)g_{2L_1} \\ &\vdots \end{aligned} \quad (67)$$

It then follows that under this generating set (ordered in the above manner), μ_1 admits a

matrix representation of the following form:

$$A_1(\sigma_1) = \begin{bmatrix} A_{1,\text{block}}(\sigma_1) & 0 & \cdots & 0 \\ 0 & A_{1,\text{block}}(\sigma_1) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{1,\text{block}}(\sigma_1) \end{bmatrix},$$

where $A_{1,\text{block}}(\sigma_1) \in \mathcal{A}_d^{L_1 \times L_1}$ is given by

$$A_{1,\text{block}}(\sigma_1) = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{1,0}(\sigma_1) & -a_{1,1}(\sigma_1) & -a_{1,2}(\sigma_1) & \cdots & -a_{1,L_1-1}(\sigma_1) \end{bmatrix}.$$

Note that $\det(A_{1,\text{block}}) = a_{1,0}(\sigma_1)$, a unit in \mathcal{A}_d . Therefore, $A_{1,\text{block}}$ is unimodular over \mathcal{A}_d . Hence, so is $A_1(\sigma_1)$.

We can further claim that not only the map μ_1 , in fact, every one of the maps $\mu_2, \mu_3, \dots, \mu_{n-d}$ has matrix representations under the chosen generating set each of which are unimodular over \mathcal{A}_d . In order to show this let us consider an $i \in \{1, 2, \dots, n-d\}$. Now, we do the following trick: we reorder the elements of \mathcal{G} so that now once again they are in descending order with a different lexicographic ordering, namely, $\sigma_{d+i} \prec \sigma_{d+1} \prec \sigma_{d+2} \prec \cdots \prec \sigma_n$. Once again, we number the elements of $\bar{\mathcal{G}}$ in this order as $\{g'_1, g'_2, \dots, g'_L\}$ where $L = \prod_{i=1}^{n-d} L_i$. Now, following exactly the same logic as above we obtain the fact that under this generating set (with this new ordering), the map μ_i admits a matrix representation of the form:

$$\tilde{A}_i(\sigma_1) = \begin{bmatrix} A_{i,\text{block}}(\sigma_1) & 0 & \cdots & 0 \\ 0 & A_{i,\text{block}}(\sigma_1) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{i,\text{block}}(\sigma_1) \end{bmatrix},$$

where $A_{i,\text{block}}(\sigma_1) \in \mathcal{A}_d^{L_i \times L_i}$ is given by

$$A_{i,\text{block}}(\sigma_1) = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{i,0}(\sigma_1) & -a_{i,1}(\sigma_1) & -a_{i,2}(\sigma_1) & \cdots & -a_{i,L_i-1}(\sigma_1) \end{bmatrix}.$$

Therefore, because $a_{i,0}(\sigma_1)$ is a unit in \mathcal{A}_d , it follows that $A_{i,\text{block}}(\sigma_1)$ is unimodular over \mathcal{A}_d . Hence, $\tilde{A}_i(\sigma_1)$ is also unimodular over \mathcal{A}_d . Now note that the new generating set $\{g'_1, g'_2, \dots, g'_L\}$ is related with the old generating set $\{g_1, g_2, \dots, g_L\}$ by a permutation. Let P_i be the corresponding *permutation matrix*. That is,

$$\begin{bmatrix} g'_1 \\ g'_2 \\ \vdots \\ g'_L \end{bmatrix} = P_i \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_L \end{bmatrix}.$$

Then, clearly, $P_i^{-1} \tilde{A}_i(\sigma_1) P_i =: A_i(\sigma_1)$ is a matrix representation of the map μ_i under the old generating set $\{g_1, g_2, \dots, g_L\}$. The unimodularity of $A_i(\sigma_1)$ then easily follows from the fact that $\tilde{A}_i(\sigma_1)$ is unimodular.

Case 2 (general q): When $q > 1$ every element in \mathcal{A}^q can be written as

$$r_1(\sigma)e_1 + r_2(\sigma)e_2 + \cdots + r_q(\sigma)e_q,$$

where $r_i(\sigma) \in \mathcal{A}$ for all i , and e_j 's are the standard basis row-vectors of \mathcal{A}^q . Recall that $\mathcal{A}^q/\mathcal{R}$ has been assumed to be a finitely generated module over \mathcal{A}_d . By Statement 3 of Lemma 39 then it follows that for every $1 \leq i < n - d$ there exists a polynomial $p_i(\sigma) \in \mathcal{A}$ of the form

$$\sigma_{d+i}^{L_i} + a_{i,L_i-1}(\sigma_1)\sigma_{d+i}^{L_i-1} + \cdots + a_{i,1}(\sigma_1)\sigma_{d+i} + a_{i,0}(\sigma_1), \quad (68)$$

where L_i is a finite positive integer, $a_{i,j}(\sigma_1) \in \mathcal{A}_d$ for all $1 \leq i \leq n - d$ and $1 \leq j \leq L_i - 1$, with $a_{i,0}(\sigma_1)$ a unit for all $1 \leq i \leq n - d$, such that

$$p_i(\sigma)e_j \in \mathcal{R} \quad (69)$$

for all $1 \leq j \leq q$. Suppose we define, like Case 1, the set of monomials

$$\mathcal{G} := \left\{ \prod_{i=1}^{n-d} \sigma_{d+i}^{\nu_i} \mid 0 \leq \nu_i \leq L_i - 1 \right\}.$$

Then, by equations (68) and (69), it follows that for every $1 \leq i \leq q$, $r_i(\sigma)e_i$ is congruent modulo \mathcal{R} to an \mathcal{A}_d -linear combination of elements in \mathcal{G} times e_i . In other words, if we define the following set

$$\mathcal{G}_{\text{vec}} := \{me_j \mid m \in \mathcal{G}, 1 \leq j \leq q\},$$

then the images of \mathcal{G}_{vec} under the canonical map $\mathcal{A}^q \twoheadrightarrow \mathcal{A}^q/\mathcal{R}$ is a generating set for $\mathcal{A}^q/\mathcal{R}$ as a module over \mathcal{A}_d . Now, notice that, under this generating set, the map μ_i is represented by a matrix

$$A_{i,\text{vec}} = \begin{bmatrix} A_i & 0 & \cdots & 0 \\ 0 & A_i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_i \end{bmatrix},$$

where A_i is the representation of $\mu_i|_{e_j}$. By Case 1, A_i is unimodular. And hence, so is $A_{i,\text{vec}}$.

Part (3) Note that if $A_i(\sigma_1)$'s are invertible then the following diagram commutes:

$$\begin{array}{ccc} \mathcal{A}_d^r & \xrightarrow{\psi} & \mathcal{M} \\ A_i(\sigma_1)^{-1} \downarrow & & \downarrow \mu_i^{-1} \\ \mathcal{A}_d^r & \xrightarrow{\psi} & \mathcal{M} \end{array} \quad (70)$$

Repeated application of Lemma 3 along with equation (70) proves that the diagram of equation (17) commutes.

Part (4) This assertion follows from Part (3).

References

- [AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley publishing Co., 1969.
- [Bjö79] J.-E. Björk. *Ring of Differential Operators*. North-Holland Publishing Company, 1979.
- [Bos82] N.K. Bose. *Applied Multidimensional Systems Theory*. Van Nostrand Reinhold, 1982.
- [CZ95] R.F. Curtain and H.J. Zwart. *An Introduction to Infinite Dimensional Linear Systems Theory*. Springer-Verlag, 1995.

- [Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, 1995.
- [FRZ93] E. Fornasini, P. Rocha, and S. Zampieri. State space realization of 2-D finite-dimensional behaviours. *SIAM Journal on Control and Optimization*, 31(6):1502–1517, November 1993.
- [KR00] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 2*. Springer-Verlag, 2000.
- [NRR11] D. Napp, P. Rapisarda, and P. Rocha. Time-relevant stability of 2D systems. *Automatica*, 47(11):2373 – 2382, 2011.
- [Obe90] U. Oberst. Multidimensional constant linear systems. *Acta Appl. Math.*, 20:1–175, 1990.
- [Par04] H. Park. Symbolic computation and signal processing. *Journal of Symbolic Computation*, 37:209–226, 2004.
- [PP13] D. Pal and H. K. Pillai. Representation formulae for discrete 2D autonomous systems. *SIAM Journal on Control and Optimization*, 51(3):2406–2441, 2013.
- [PQ99] J-F. Pommaret and A. Quadrat. Localization and parametrization of linear multidimensional control systems. *Systems and Control Letters*, 37:247–260, 1999.
- [PS98] H. K. Pillai and S. Shankar. A behavioral approach to control of distributed systems. *SIAM Journal on Control and Optimization*, 37(2):388–408, 1998.
- [PWR02] H. K. Pillai, J. Wood, and E. Rogers. On homomorphisms of n-D behaviors. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, 49(6):732 –742, june 2002.
- [RW89] P. Rocha and J. C. Willems. State for 2-D systems. *Linear Algebra and its Applications*, 122/123/124:1003–1038, 1989.
- [RW97] Paolo Rapisarda and J. C. Willems. State maps for linear systems. *SIAM Journal on Control and Optimization*, 35(3):1053–1091, May 1997.
- [Stu02] B. Sturmfels. *Solving Systems of Polynomial Equations*. American Mathematical Society with support from the National Science Foundation, 2002.
- [STW02] A. J. Sasane, E. G. F. Thomas, and J. C. Willems. Time autonomy versus time controllability. *Systems and Control Letters*, 45:145–153, 2002.
- [Swa78] R. Swan. Projective modules over Laurent polynomial rings. *Transactions of the AMS*, 237:111–120, March 1978.
- [Val01] M. E. Valcher. Characteristic cones and stability properties of two-dimensional autonomous behaviors. *IEEE Transactions on Circuits and Systems–Part I: Fundamental Theory and Applications*, 47(3):290–302, 2001.
- [Wil83] J. C. Willems. Input-output and state-space representations of finite dimensional linear time-invariant systems. *Linear Algebra and its Applications*, 50:581–608, 1983.
- [Wil91] J. C. Willems. Paradigms and puzzles in the theory of dynamical systems. *IEEE Transactions on Automatic Control*, 36(3):259–294, March 1991.

- [Zam98] S. Zampieri. Causal input/output representation of 2D systems in the behavioral approach. *SIAM Journal on Control and Optimization*, 36(4):1133–1146, July 1998.
- [Zer99] E. Zerz. Primeness of multivariate polynomial matrices. *Systems and Control Letters*, 29:139–145, 1999.